

Desde nuestros sistemas se puede acceder a los siguientes Web Service de Afip:

WSFE – Web Service de Factura Electrónica

WSFEX- Web Service de Factura Electrónica de Exportación

WSBFE – Web Service de Factura Electrónica bonos fiscales y bienes de capital

WSMTXCA – Web Service Factura Electrónica con Detalle

WSCTG – Web Service Código de Trazabilidad de Granos

WSLPG - Web Service - Liquidación Primaria de Granos

Para poder trabajar con los Web Service de Afip, previamente se debe generar un certificado digital por medio de un utilitario llamada OpenSSL, y luego hacer autorizar ese certificado por la AFIP. Se presupone que ya se posee clave fiscal de nivel acorde a los servicios que se utilizan (NIVEL 3), tramitada en una dependencia de AFIP. A continuación se describen los pasos para crear y autorizar el certificado.

PASO1: Bajar e instalar el Visual C++ redistribuible, que es un requisito previo a la instalación del OPENSSL. Se puede bajar desde nuestra página web www.aeayasoc.com :

Dentro de la página, ir a Resoluciones:



Ahí hacer click sobre:

- **Microsoft Visual C++ 2008 Redistributable Package (x86)** (si el Windows que ustedes poseen es de 32 bits).
- **Microsoft Visual C++ 2008 Redistributable Package (x64)** (si el Windows que ustedes poseen es de 64 bits).

aeayasoc.com Cel. +54 (341)155-112898 (Las 24 horas los 365 días del año)

Inicio Sistemas Actualizaciones Novedades Aplicativos Resoluciones Comunicarse con... Buscar

Resoluciones

Nuestra Empresa

Informar Pagos

Contactos

Eventos

Links de Interes

Sitios Agropecuarios y Noticias
Bolsas de Comercios
Clima
Acopios y Acondicionadores
Corredores de Cereales

Entidades del gobierno

Afip
Oncca
Afip (Consulta al Registro Fiscal de Operadores)
Secretaría de Agricultura Ganadería y Pesca (SAGPyA)
I.N.D.E.C

Rosario

SANTA FE

20°C
H 72%

Pr. 1013hP
Ind.UV 10

Resolución General AFIP 3419/2012 Liquidación Primaria Electrónica de Datos

Resolución General AFIP 3339/2012 Programa Movimientos de Granos 4.0

Resolución General AFIP 3100/2011

Resolución General AFIP 3060/2011

Decreto Presidencial 192/2011

Resolución General AFIP 3034/2011

Resolución General AFIP 2975/2010

Resolución General AFIP 2809/2010

Resolución General Conjunta AFIP 2773/2010

Resolución General AFIP 2596/2009

Resolución Oncca 1962/2006 Modificación de la Disposición 5338/2005

Resolución General AFIP 3342/2012 Régimen informativo existencias granos.

Resolución General AFIP 3292/2012 Tarifa Flete en Carta Porte

Resolución General AFIP 3061/2011

Resolución Conjunta MAGPA 106/2011, MI 74/2011 y MEPP 57/2011

Resolución General AFIP 3036/2011

Resolución Conjunta AFIP 2976/2010 y ONCCA 737/2010

Resolución General AFIP 2853/2010

Resolución General AFIP 2806/2010

Resolución General AFIP 2616/2009

Resolución AFIP 7953/2008

Resolución General AFIP 3419/2012

20/12/2012. Operaciones de compraventa de granos no destinados a la siembra. Régimen de emisión de comprobantes. Liquidación primaria electrónica de datos.

[Instrucciones para generar certificado digital Afip](#)

Microsoft Visual C++ 2008 Redistributable Package (x86)

Microsoft Visual C++ 2008 Redistributable Package (x64) (Windows 64 bits)

OpenSSL-0_9_8i.exe

Certificado Confianza Sitio Afip

Una vez que se hace click sobre algunos de estos ítems, vemos la siguiente ventana:

Microsoft Sign in

Download Center

Products Categories Security Support

Microsoft Visual C++ 2008 Redistributable Package (x86)

Quick links

- Overview
- System requirements
- Instructions

Looking for support?

Visit the Microsoft Support site now >

The Microsoft Visual C++ 2008 Redistributable Package (x86) installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ on a computer that does not have Visual C++ 2008 installed.

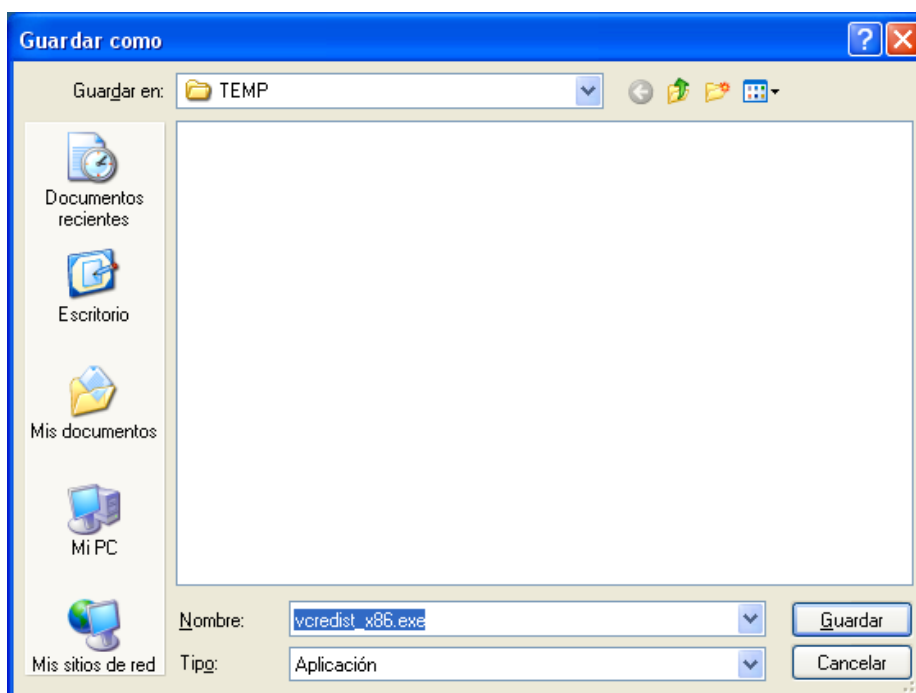
Quick details

Version:	x86	Date published:	11/29/2007
Change language:	English		
File name	Size		
vcredist_x86.exe	1.7 MB		DOWNLOAD

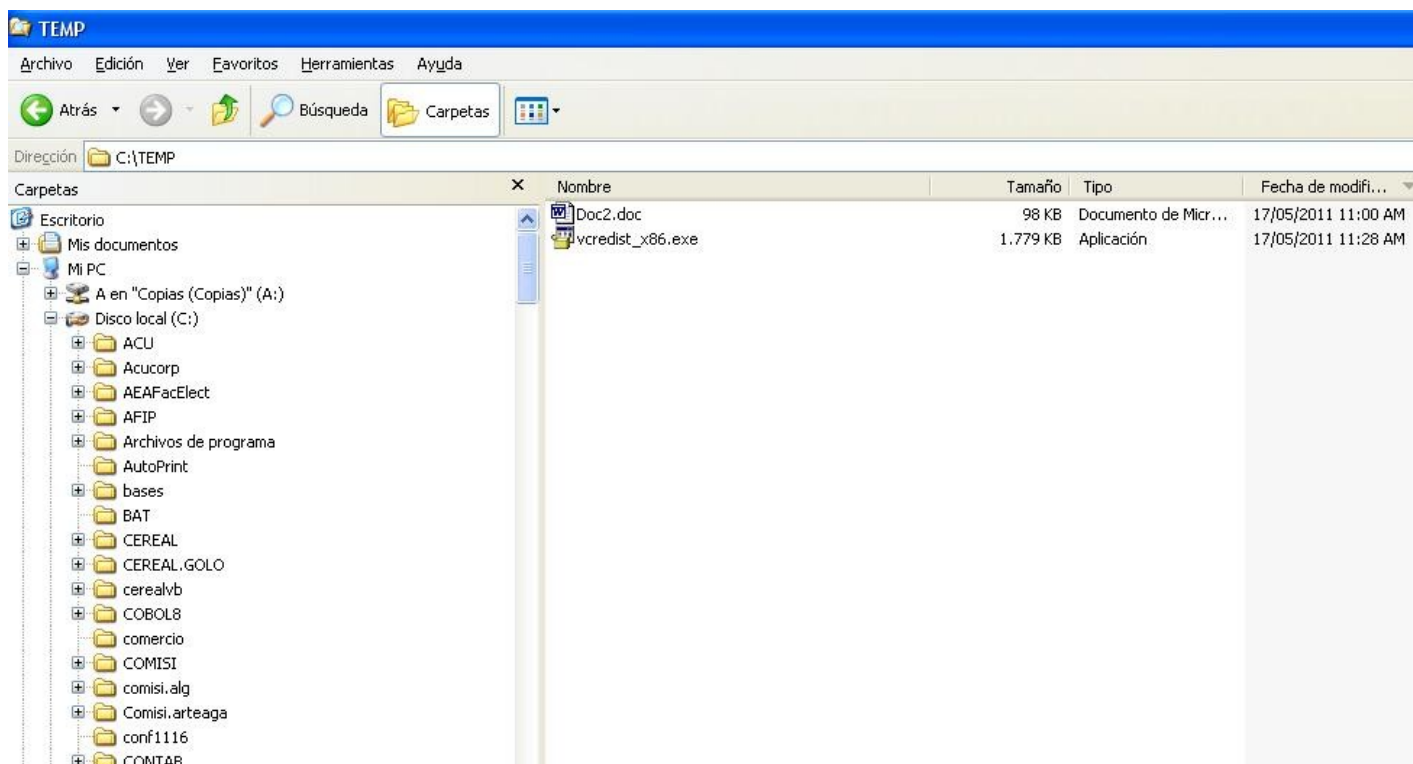
Hacemos click en “Download” y vemos una ventana parecida a la siguiente:



Hacemos click en “Guardar” y seleccionamos una carpeta temporal donde guardar el archivo de instalación del Visual C++ redistribuible, como se ve aquí (en el ejemplo se utiliza la carpeta TEMP):

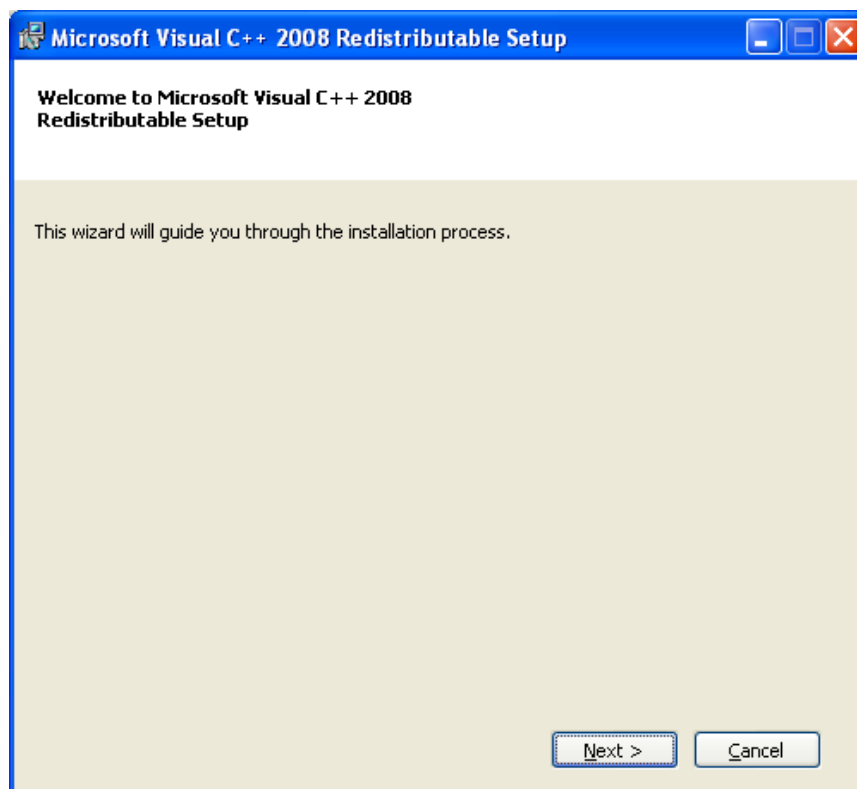


Luego en una ventana de “Mi PC” ingresamos a la carpeta elegida y ejecutamos con doble click el archivo de nombre **vcredist_x86.exe**:

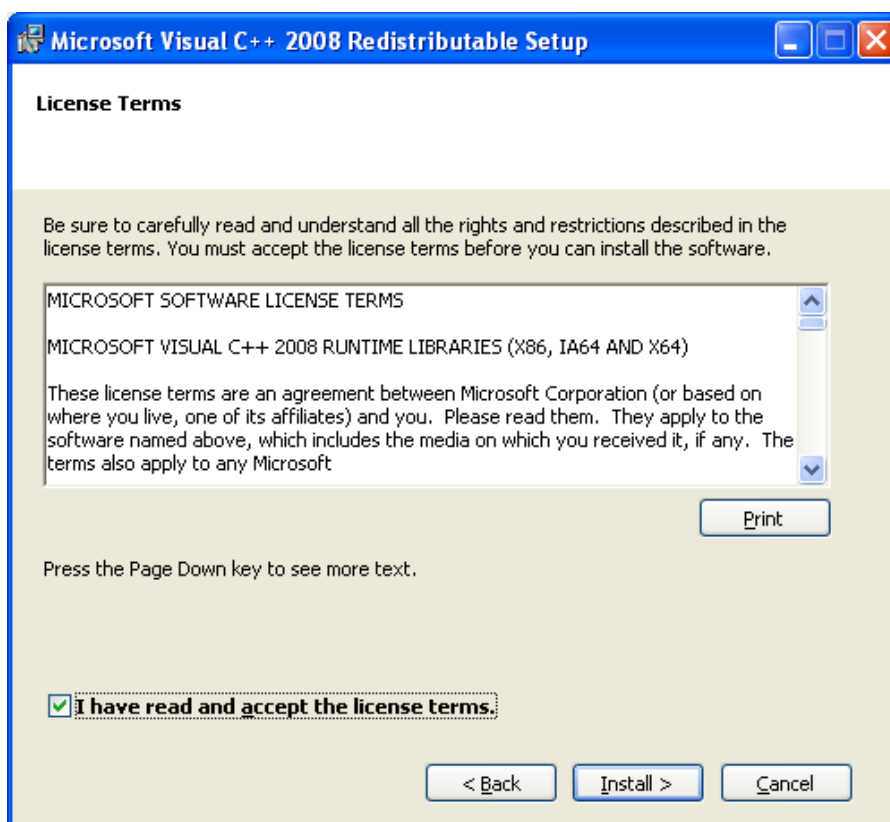


Al comenzar la instalación del Visual C++ redistribuible, lo primero que podemos observar es una advertencia, hacer click en el botón “Ejecutar”, luego vemos la pantalla de presentación de la instalación:

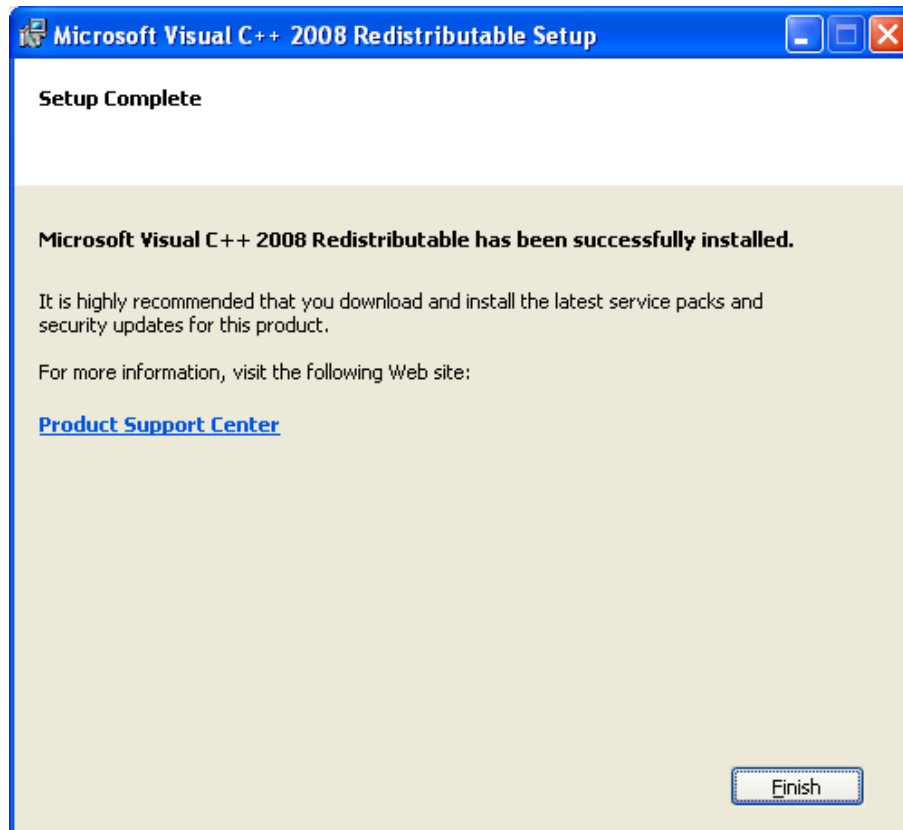




Hacer click en “Next” para continuar, así vemos la próxima ventana:



Tildar la casilla “I have read and accept the license terms” y hacer click en “Install”. Luego veremos la siguiente ventana:



Hacer click en “Finish” para terminar la instalación.

PASO2: Bajar e instalar OpenSSL para Windows. Se puede bajar desde nuestra página web www.aeayasoc.com :

Dentro de la página, ir a Resoluciones:

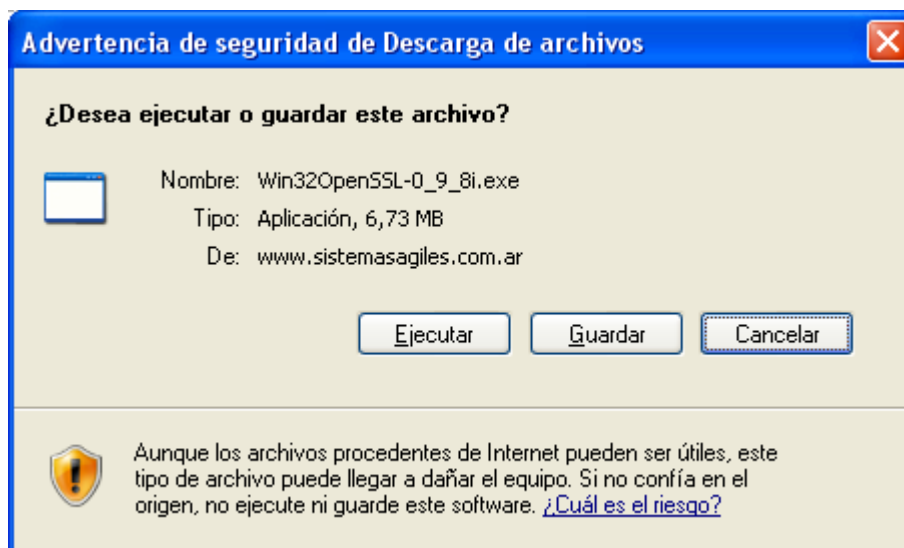


Ahí hacer click sobre:

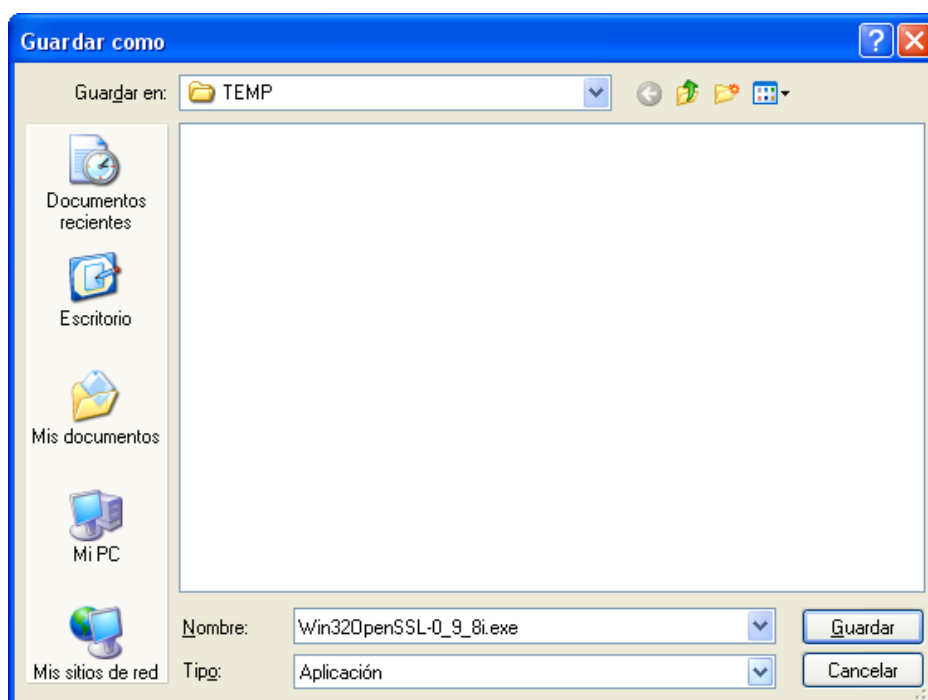
- [OpenSSL-0_9_8i.exe](#).



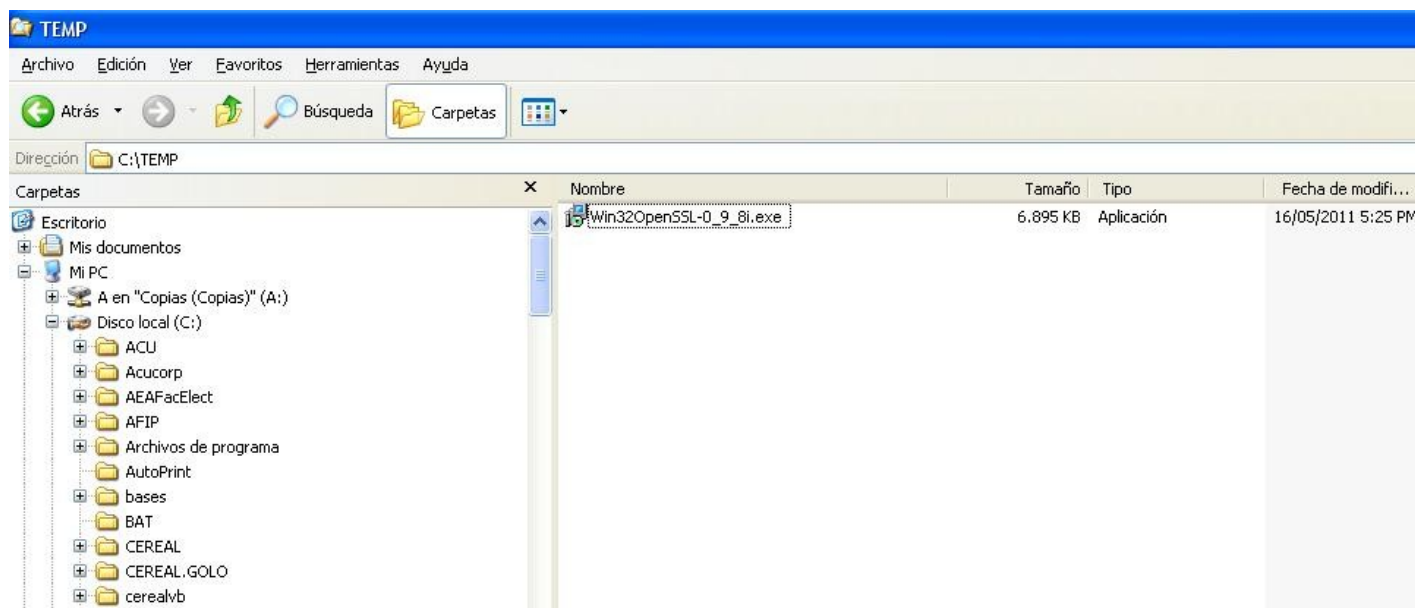
Una vez ejecutado el vínculo, automáticamente vamos a ver una ventana similar a la siguiente:



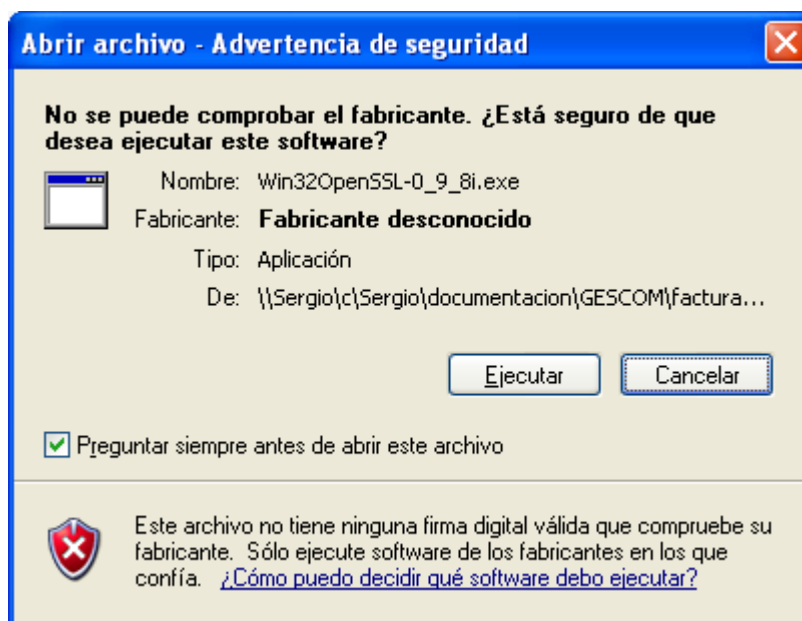
Hacer click en el botón “Guardar”, y elegir como destino alguna carpeta temporal de la PC, como se ve en el siguiente ejemplo (se usa TEMP), luego click nuevamente en el botón “Guardar”:



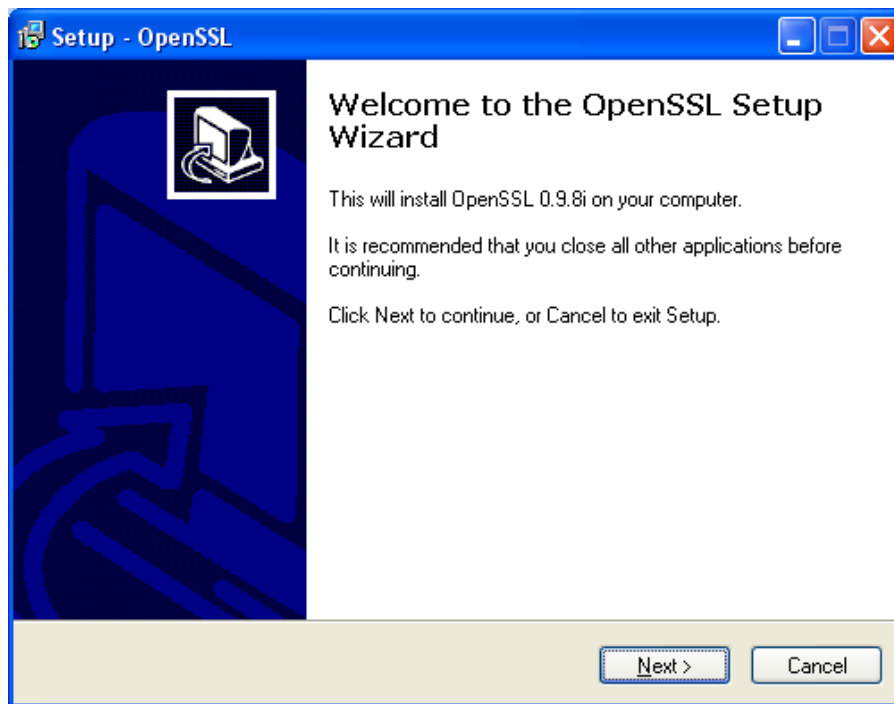
Abrir una ventana de “Mi PC”, ingresar a la carpeta temporal donde guardamos el archivo, y ejecutar con doble click el que tiene el nombre **Win32OpenSSL-0_9_8i.exe**



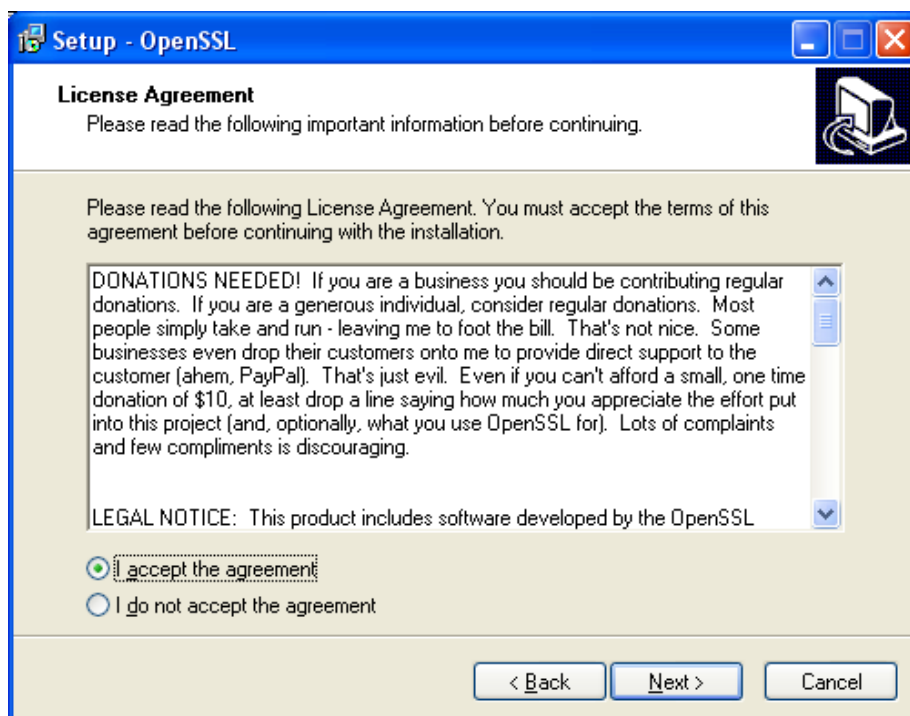
Al comenzar la instalación del OPENSSL, lo primero que podemos ver es la ventana de advertencia de Windows, si es así, hacer clic en el botón “ejecutar” y continuar con la instalación.



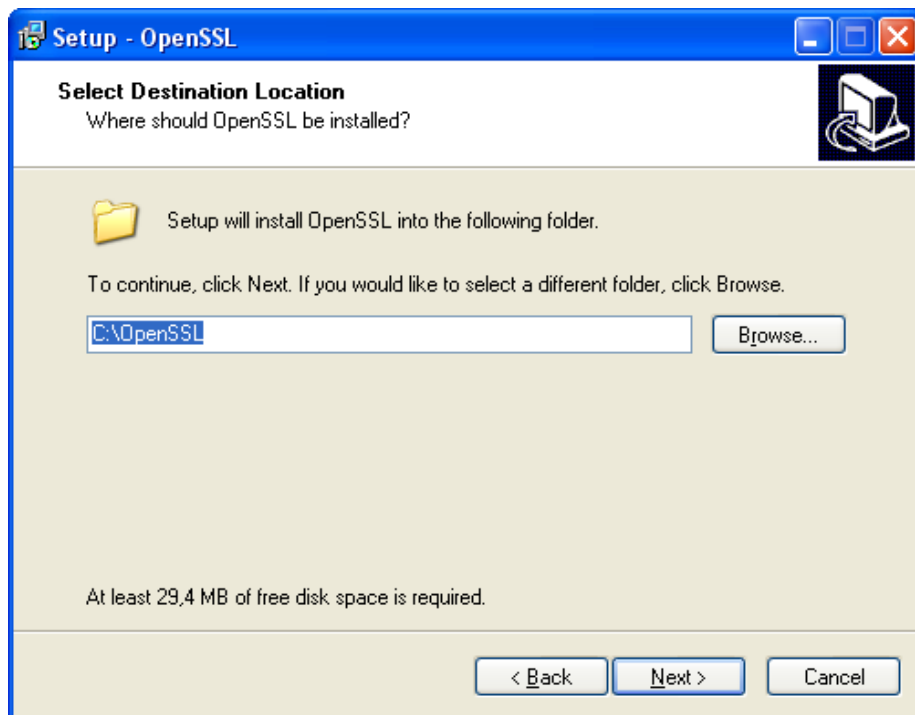
Luego vamos a observar la pantalla de presentación de la instalación del OPENSSL, como se ve a continuación:



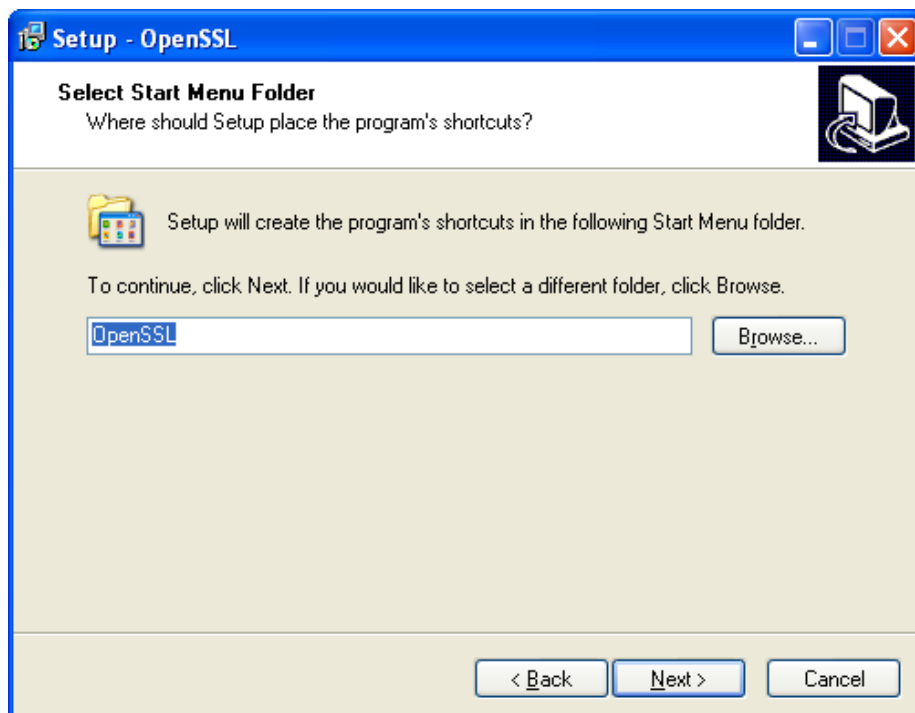
Al hacer click en el botón “Next”, aparece una ventana como la siguiente:



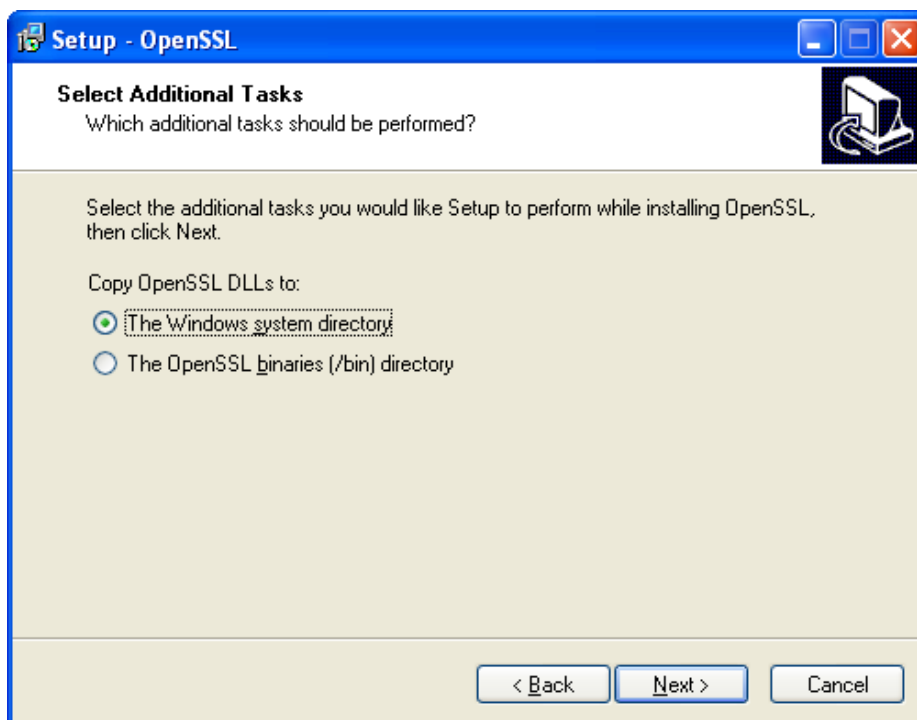
Tildar la opción “I accept the agreement” y hacer click nuevamente en el botón “Next” para ver la siguiente ventana:



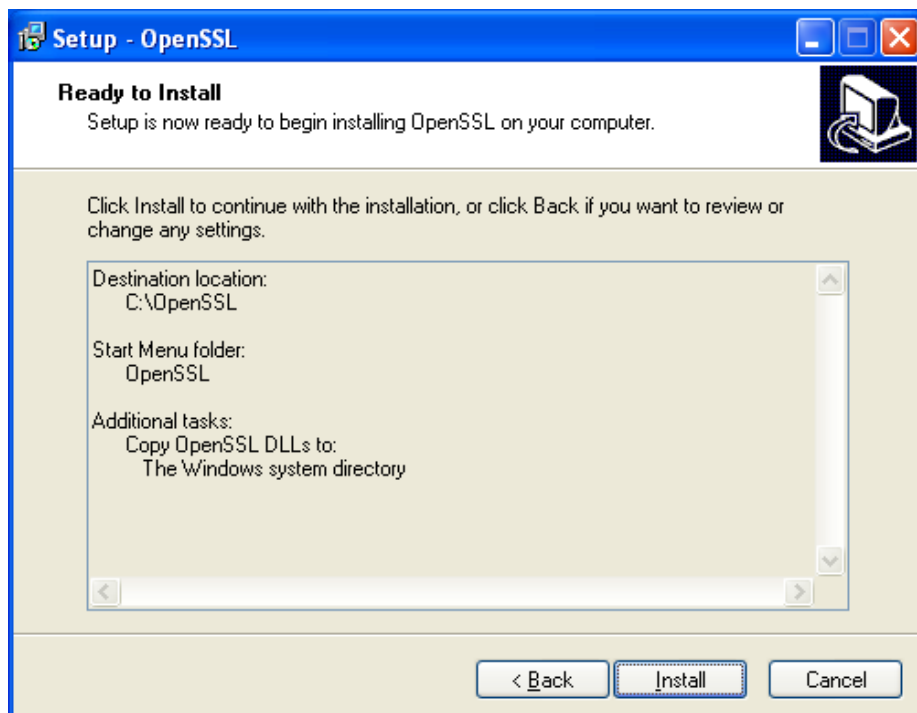
Dejar como carpeta destino para la instalación la que propone la ventana, y hacer click en el botón “Next”.
Vemos la siguiente ventana:



Dejar lo que propone y hacer click en “Next” para ver la siguiente ventana:

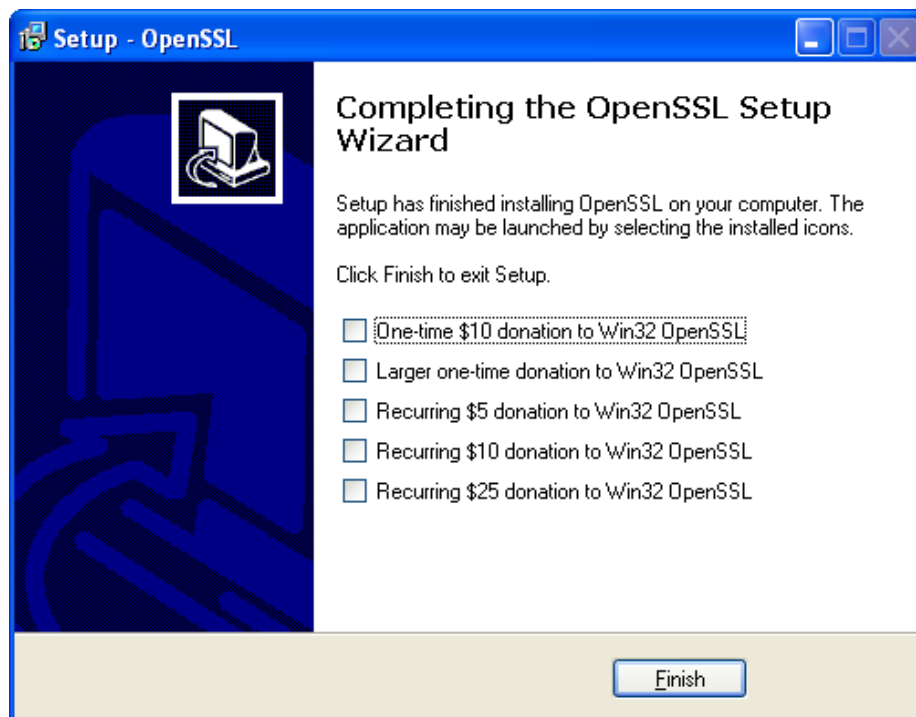


Dejar el valor que propone, es decir el tilde en “The Windows system directory”, hacer click en “Next” . Vamos a ver la última ventana de la instalación, que es una confirmación de todo lo seleccionado previamente:



Hacer click en el botón “Install” para finalizar la instalación.

Si al finalizar aparece la siguiente ventana, asegurarse de destildar todas las opciones, como se ve en nuestro ejemplo:



Luego hacer clic en “Finish” para completar el proceso.

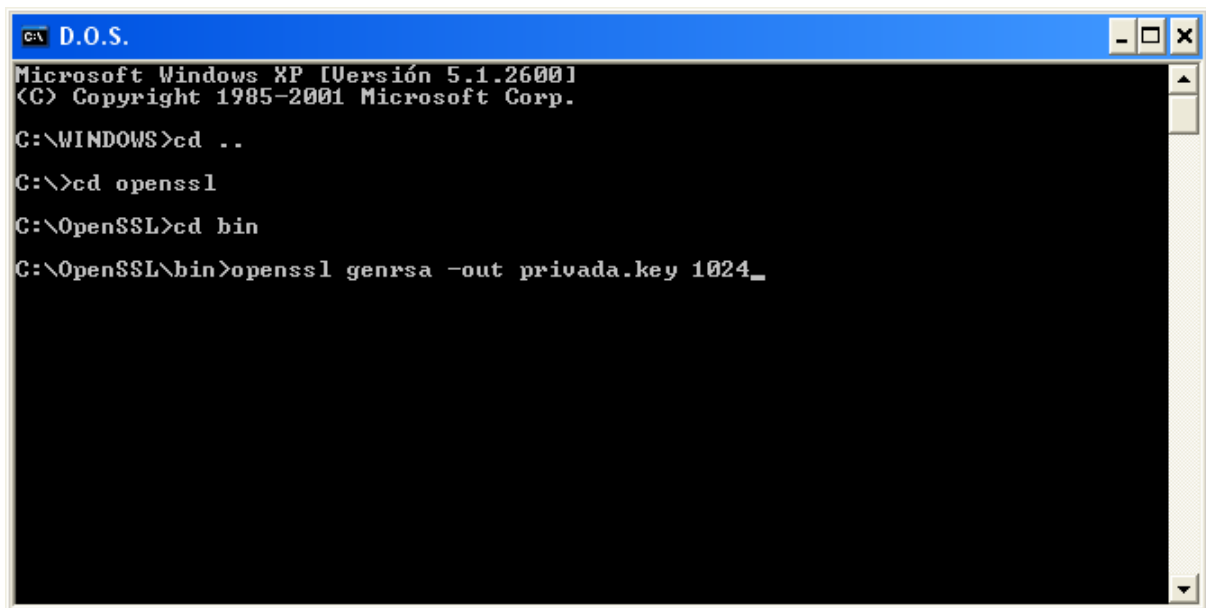
PASO3: Una vez instalados los programas necesarios, el próximo paso será generar el certificado digital. Para tal fin, seguir las siguientes instrucciones:

- Ingresar por línea de comando (MSDOS) al directorio de OpenSSL C:\OpenSSL\bin>
Si es Windows 7 ingresar a “Símbolo del Sistema” ejecutándolo como Administrador.
- Generar la clave privada con los siguientes comandos:

```
set RANDFILE=.rnd (este se ejecuta solo si tienen windows 7,  
para que no de el error "unable to write 'random state'")
```

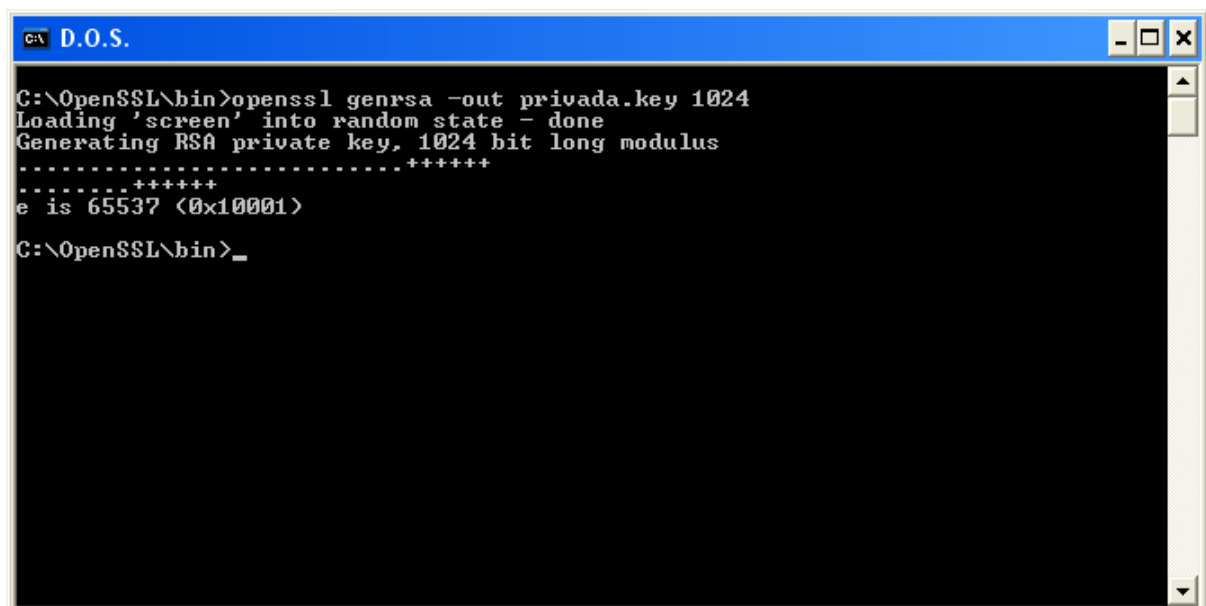
Openssl genrsa -out privada.key 1024

Aquí podemos ver un ejemplo:



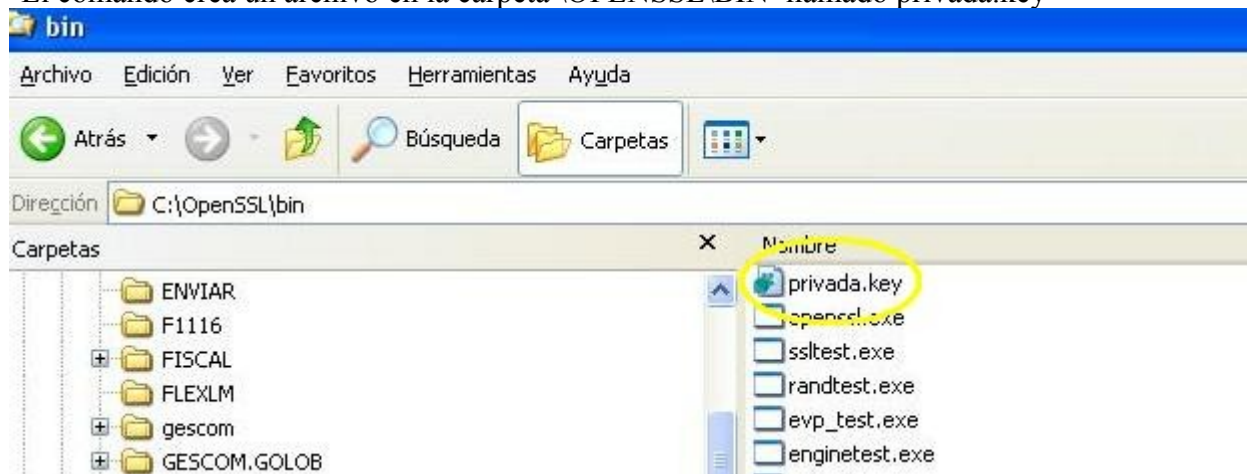
```
C:\ D.O.S.  
Microsoft Windows XP [Versión 5.1.2600]  
<C> Copyright 1985-2001 Microsoft Corp.  
C:\WINDOWS>cd ..  
C:\>cd openssl  
C:\OpenSSL>cd bin  
C:\OpenSSL\bin>openssl genrsa -out privada.key 1024_
```

Al ejecutar el comando se ve lo siguiente:



```
C:\OpenSSL\bin>openssl genrsa -out privada.key 1024  
Loading 'screen' into random state - done  
Generating RSA private key, 1024 bit long modulus  
.....++++++  
.....++++++  
e is 65537 (0x10001)  
C:\OpenSSL\bin>_
```

El comando crea un archivo en la carpeta \OPENSSL\BIN llamado privada.key



OBS: conviene hacer un respaldo del archivo generado que contiene la clave privada (archivo llamado **privada.key** que se encuentra en \OPENSSL\BIN) para evitar futuros inconvenientes, ya que será vital para los futuros pasos y no debe faltar.

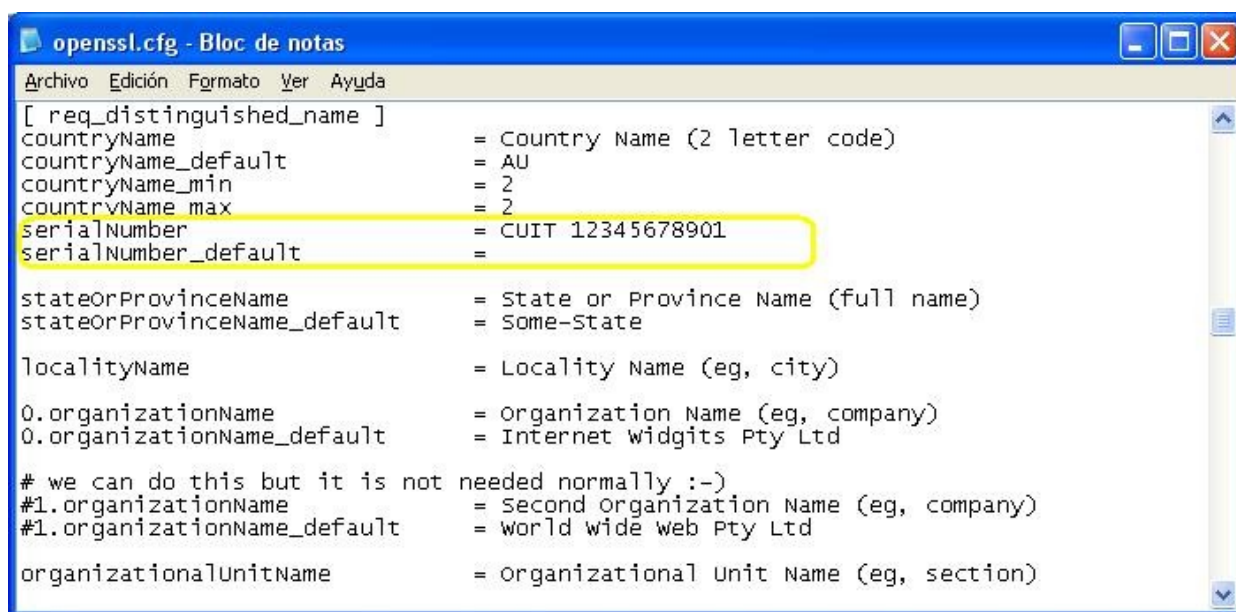
- Editar con algún editor de texto estándar el archivo C:\OpenSSL\bin\openssl.cfg:

En la sección **[req_distinguished_name]** del archivo agregar/modificar las líneas:

serialNumber = (Poner aquí la palabra CUIT seguido del numero de CUIT de la empresa)
serialNumber_default =

(OBS: Es importante que la primera letra de “serial” sea minúscula)

En la siguiente pantalla podemos ver un ejemplo de lo dicho:



Guardar los cambios y cerrar el archivo.

- Generar el pedido (CSR: certificate signing request) ejecutando desde la línea de comando:

openssl req -new -key privada.key -out pedido.csr

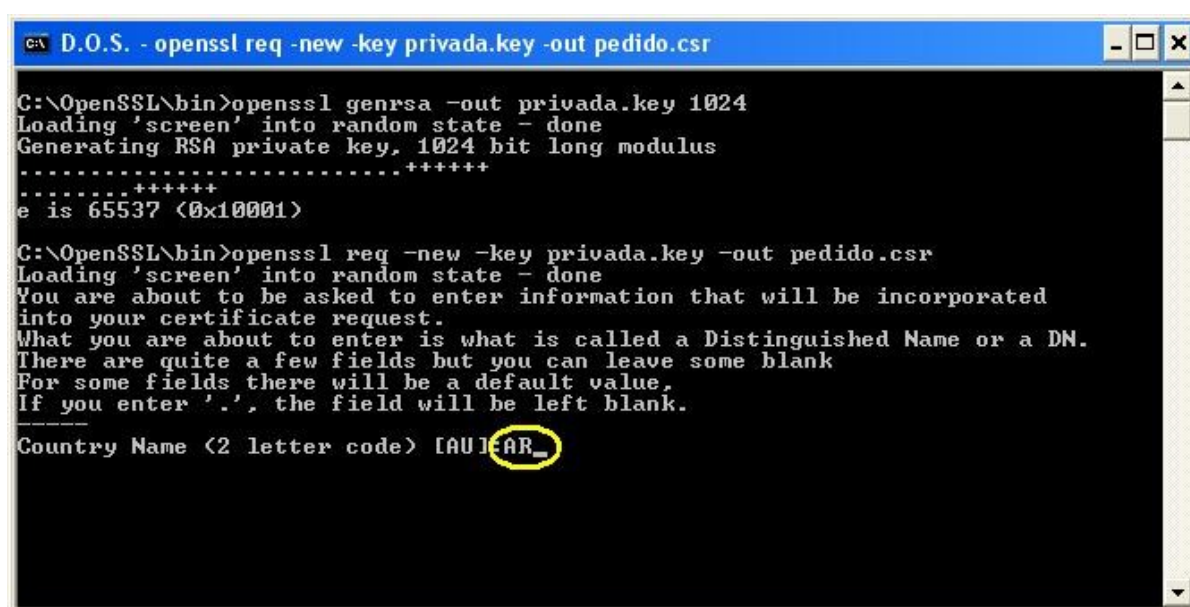
Al ejecutar el comando, nos va a solicitar por pantalla algunos datos. Los campos obligatorios son:

CountryName (AR)
SerialNumber (CUIT, sin guiones)
OrganizationName (Razón Social de la Empresa)
CommonName (Persona o Sistema)

Veamos un ejemplo:

El primero que se pide es “Country Name (2 letter code) [AR]:”

Allí tenemos que ingresar la sigla **AR** como se ve en la pantalla:



```
C:\OpenSSL\bin>openssl genrsa -out privada.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)

C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AR_
```

Luego, la aplicación solicita el número de CUIT, como se ve a continuación:

```

C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AR
CUIT 12345678901 []:

```

Ingresa la palabra CUIT, luego un espacio en blanco y finalmente el número de CUIT sin guiones.
Ejemplo: CUIT 12345678901

Los dos siguientes se pueden dejar en blanco.

Luego pide el nombre de la empresa que es obligatorio, se ve en pantalla “Organization Name”.
Debemos ingresar la razón social de la empresa tal cual figura en la consulta de inscripción en AFIP.
Ejemplo:

```

C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AR
CUIT 12345678901 []:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AEAYASOC
Common Name (eg, your name or organization) []:

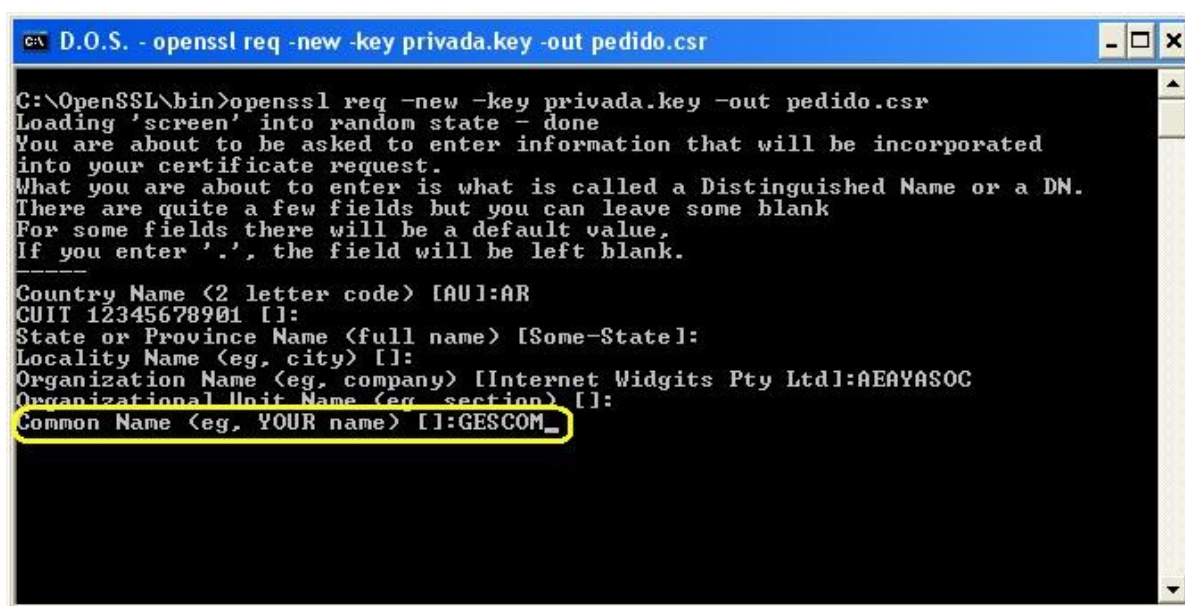
```

Luego se solicita el dato “Common Name”.

Ingresa aquí el nombre del servicio, aplicación u unidad operativa. Aquí pueden colocar el sistema que ustedes poseen:

- ✓ Agroacopio
- ✓ AgroBrokers
- ✓ Cereal
- ✓ Comisi
- ✓ Gescom

En el ejemplo se utilizó: **GESCOM**



```
C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name <2 letter code> [AU]:AR
CUIT 12345678901 []:
State or Province Name <full name> [Some-State]:
Locality Name <eg, city> []:
Organization Name <eg, company> [Internet Widgits Pty Ltd]:AEAYASOC
Organizational Unit Name <eg, section> []:
Common Name <eg, YOUR name> []:GESCOM_
```

Finalmente, se solicitan otros datos que nos son obligatorios, dejarlos en blanco, dar ENTER hasta que concluya el comando.

Una vez que haya generado correctamente su CSR, puede usarlo para obtener su certificado digital X.509.

Para el caso del entorno de Producción (entorno real) se podrá obtener el certificado interactivamente usando el servicio "Administración de Certificados Digitales" del menú de trámites con Clave Fiscal en el portal www.afip.gob.ar. (Para saber los pasos para obtener el certificado de la página de AFIP, ver **ANEXO I**).

Una vez autorizados a usar el Web Services correspondiente de AFIP, la empresa quedará registrada en el servicio de autorización de AFIP como entidad autorizada para usar el Web Services que corresponda.

Para trabajar en un entorno de pruebas, se puede generar un certificado de Homologación siguiendo los pasos del ANEXO II.

En ambos casos (Homologación o Producción) se obtiene un archivo de extensión "crt" y se puede continuar con el **PASO 4**. En caso de generar los dos certificados, prestar especial atención al nombre que se le asigna a cada archivo.

PASO 4: Una vez generado el certificado (PASO3), obtenemos un archivo con extensión *.cert. Este es el certificado a usar. Pero **ATENCIÓN** el certificado devuelto por AFIP es **extensión *.cert** y el runtime de NET y el OCX esperan un **certificado extensión *.pfx**. De lo contrario recibiremos un error de conexión similar a: "La contraseña de red especificada no es válida" o bien "la clave no existe".

Para poder usar el certificado es necesario convertirlo. A continuación se explican los pasos para convertirlo (primeramente debemos convertir el certificado *.cert a la extensión *.p12. y de esta extensión a *.pfx)

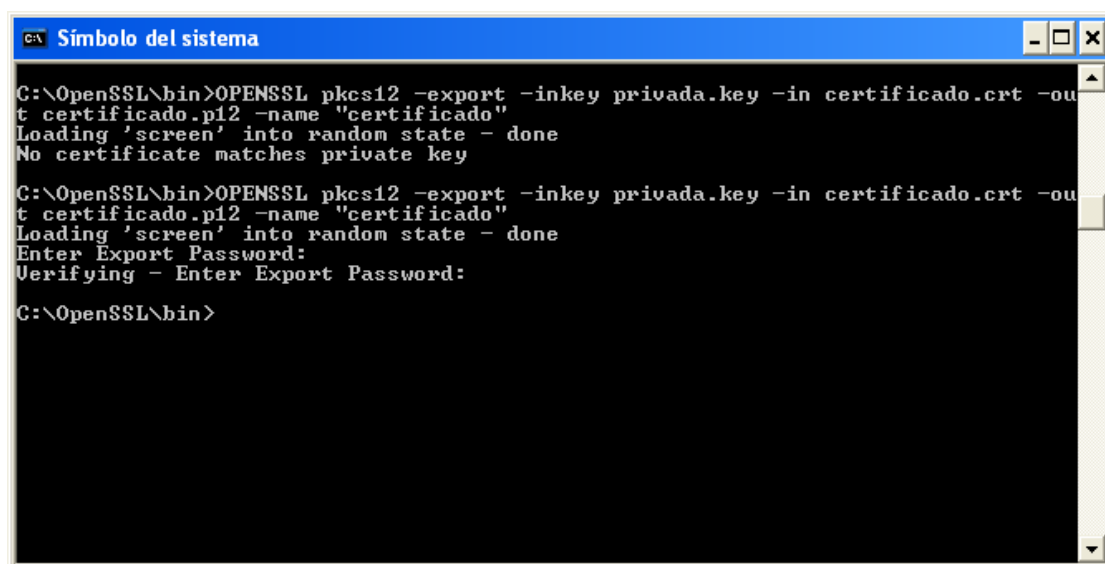
Para convertir el certificado del formato crt al formato p12 :

- Guardar el archivo *.cert enviado por AFIP en la carpeta OPENSSL\BIN
- Ingresar por línea de comando (MSDOS) al directorio de OpenSSL C:\OpenSSL\bin>
- Ejecutar el siguiente comando:

openssl pkcs12 -export -inkey privada.key -in x.cert -out x.p12 -name "x"

Reemplazando las letras x (que están en color rojo) por el nombre del certificado recibido de AFIP. Solo reemplazar las letras x, dejar comillas, guiones y puntos como están (**si al ejecutar el comando solicita una contraseña o clave no ingresar nada, pulsar Enter directamente**).

La pantalla será similar a esta:



```

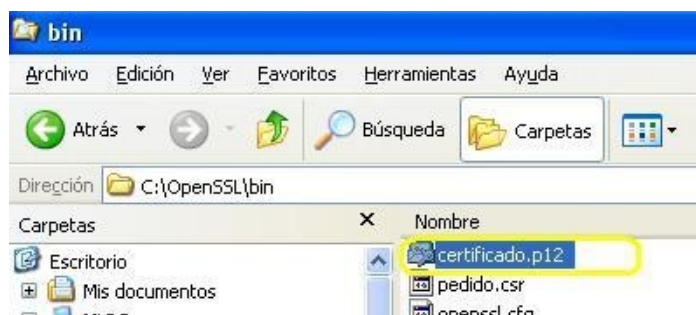
C:\OpenSSL\bin>openssl pkcs12 -export -inkey privada.key -in certificado.cert -out
t certificado.p12 -name "certificado"
Loading 'screen' into random state - done
No certificate matches private key

C:\OpenSSL\bin>openssl pkcs12 -export -inkey privada.key -in certificado.cert -ou
t certificado.p12 -name "certificado"
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL\bin>
    
```

(en este ejemplo, nuestro archivo se llama **certificado.cert** pero puede tener otro nombre)

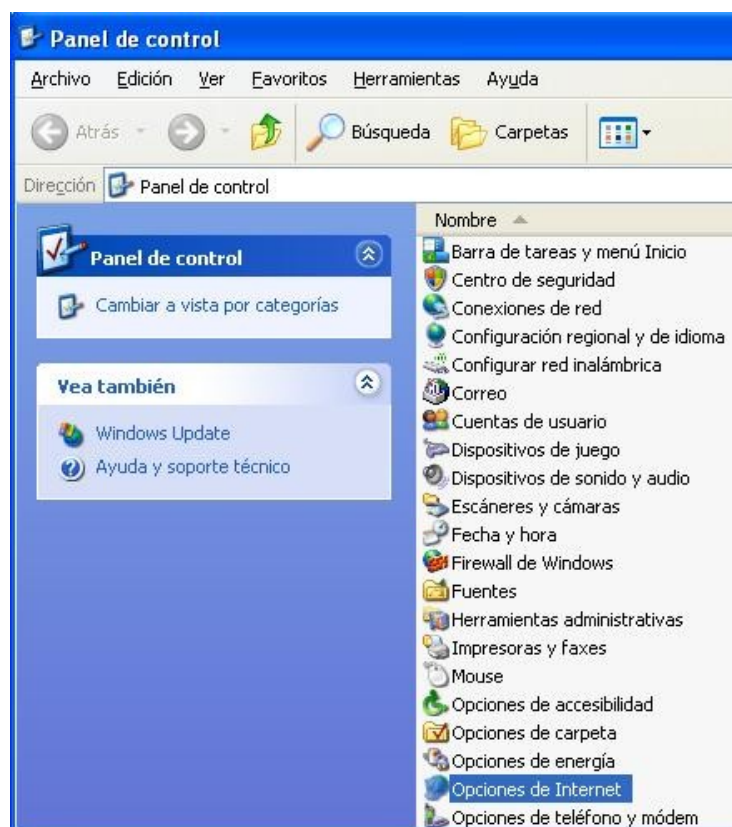
Esto nos dejará en la carpeta OPENSSL\BIN un archivo de extensión p12 como se ve en el siguiente ejemplo:



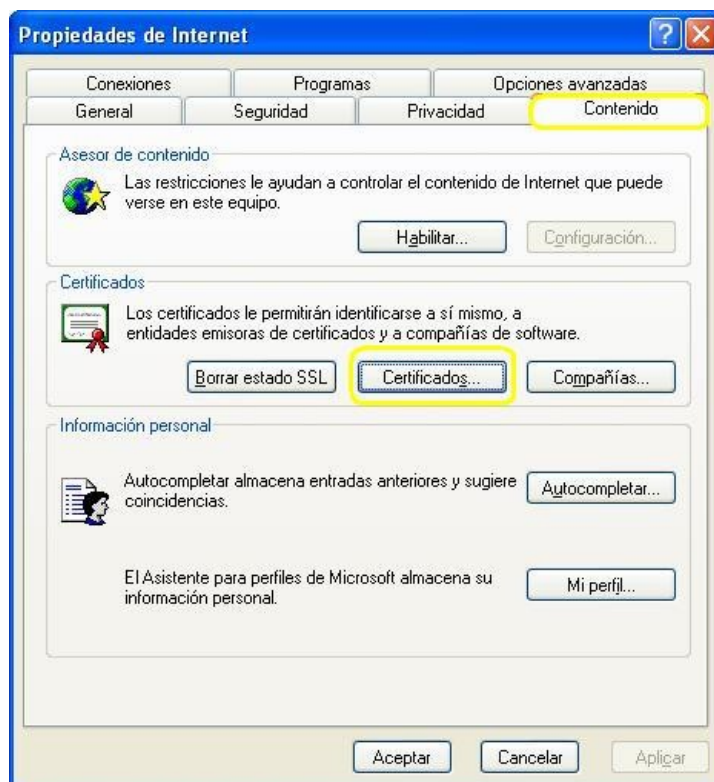
Este archivo de extensión p12 debemos convertirlo a extensión .pfx desde el panel de control.

Los pasos y las pantallas corresponden a Windows XP. En algunos Windows las pantallas son similares aunque en algunos casos (por configuración de permisos o por el control UAC) la conversión pide una contraseña. En estos casos seguir igualmente la guía pero creando una contraseña.

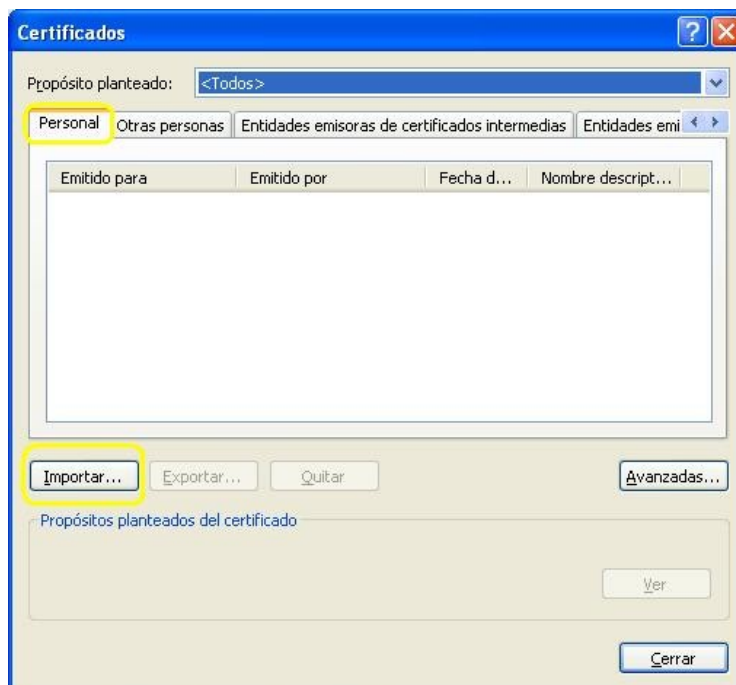
- Ir a Panel de Control.
- Ir a Opciones de Internet.



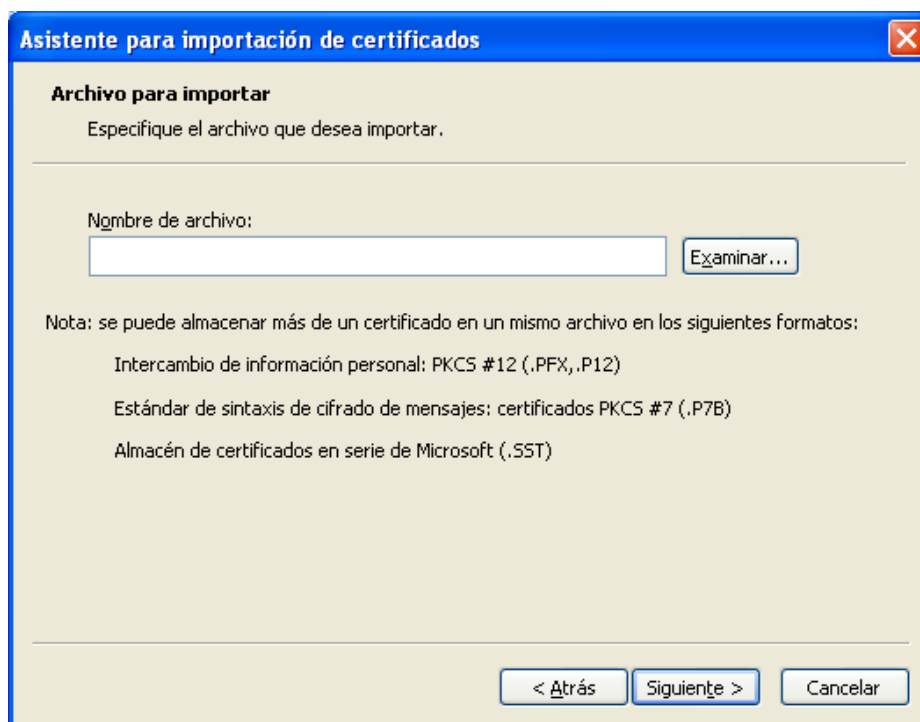
- Ir a solapa "contenido"
- Seleccionar el botón "certificados"

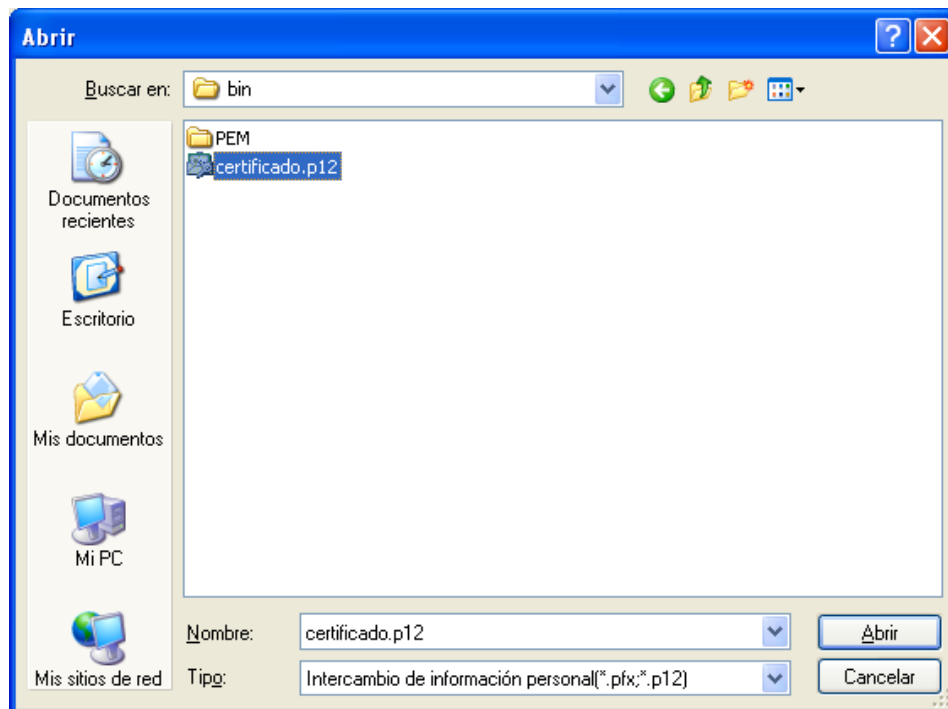


- Ir a solapa "personal" (la primera).
- Seleccionar el botón "importar".

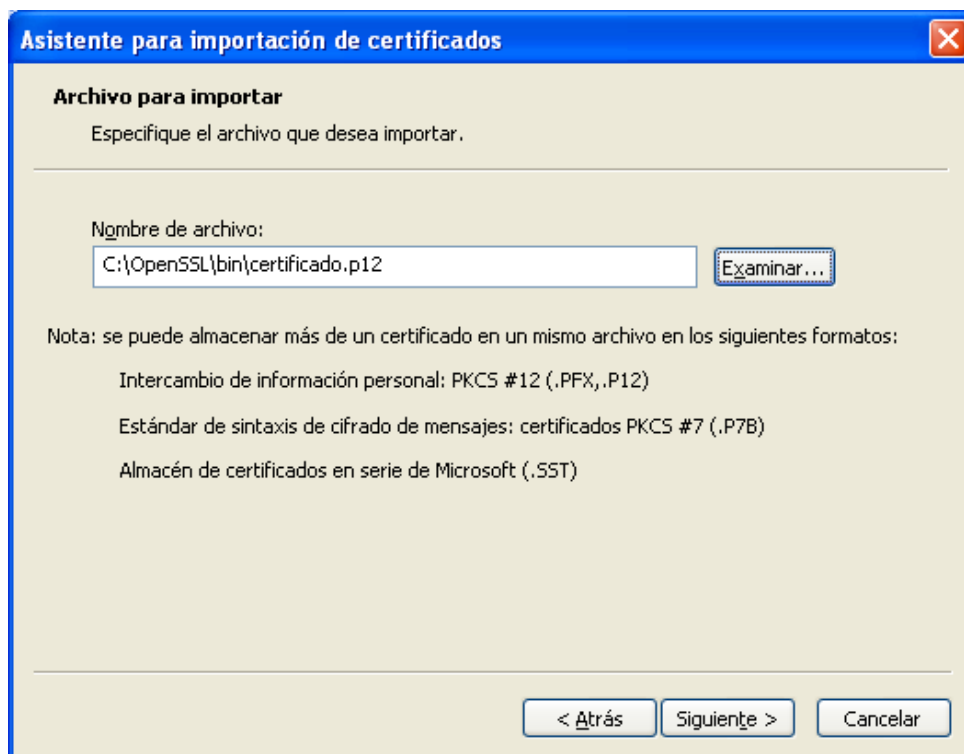


- En la pantalla del asistente seleccionar "siguiente". Nos pedirá donde está el archivo *.p12 para convertir a *.pfx. Seleccionar el botón "examinar". Antes de navegar hasta la carpeta donde está el archivo *.p12 (generalmente c:\openssl\bin) indicar en "tipo de archivo" que estamos buscando un archivo *.p12 como muestran estas pantallas:





- Seleccionar el archivo *.p12 y aceptar (en nuestro ejemplo es certificado.p12).
- En el asistente seleccionar "siguiente".



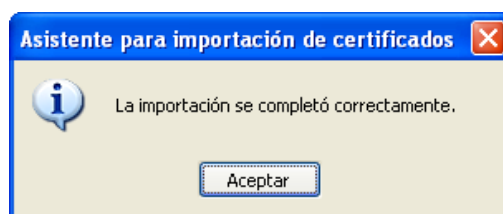
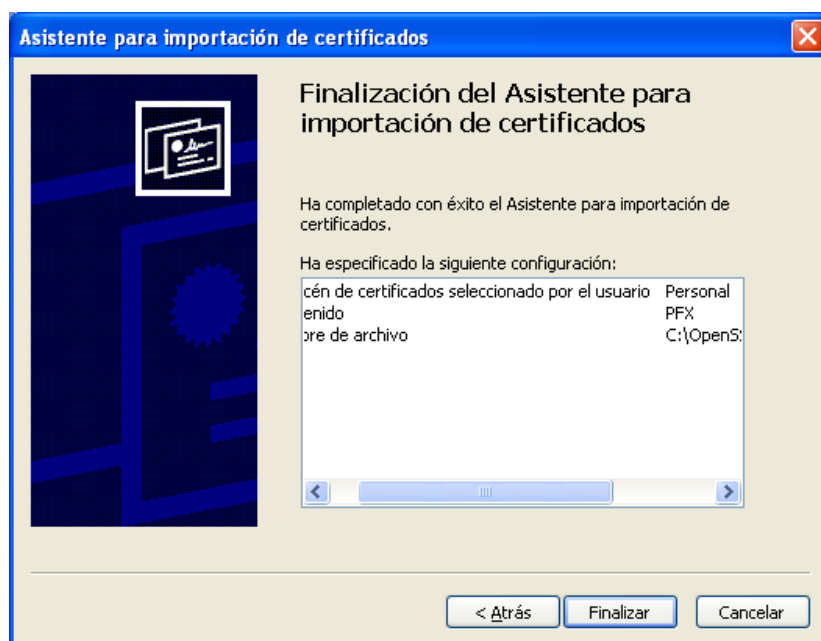
- Nos pedirá una contraseña. No colocar nada (excepto que específicamente se quiera proteger el archivo de certificados con una contraseña o el propio Windows obligue a hacerlo, en este caso, crear una contraseña y marca como exportable). Debe quedar algo como esto:

The screenshot shows the 'Asistente para importación de certificados' window with the 'Contraseña' tab selected. The text reads: 'Para mantener la seguridad, la clave privada se protege con una contraseña.' Below this, it says 'Escriba la contraseña para la clave privada.' There is a text box labeled 'Contraseña:' which is empty. Below the text box, there are two checkboxes: 'Habilitar protección segura de claves privadas. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.' (unchecked) and 'Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.' (checked). At the bottom, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'.

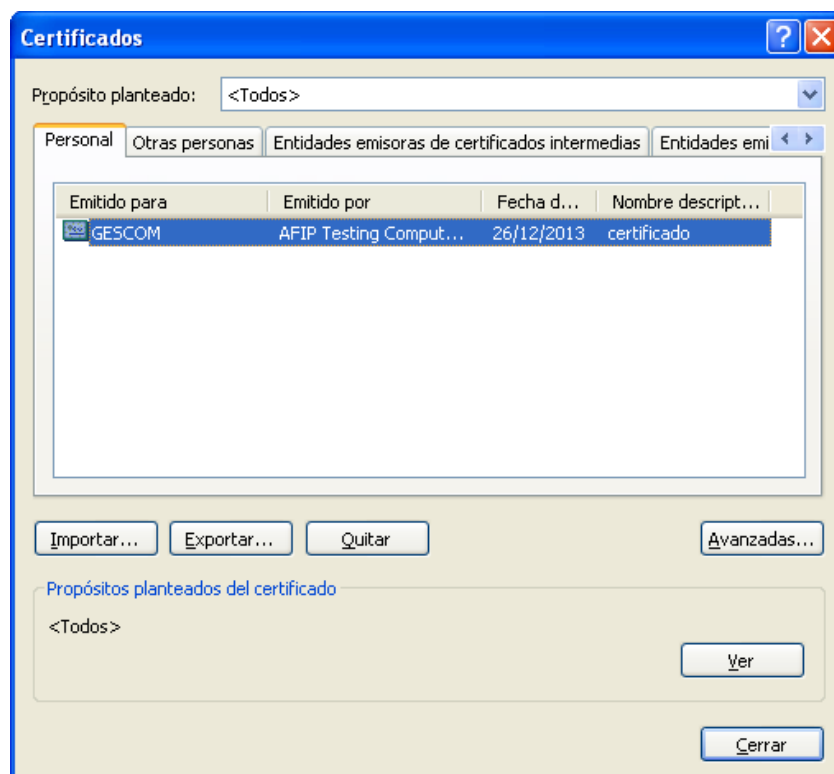
- Seleccionar "Siguiente". Nos pedirá en que lugar se guarda el certificado. Dejarlo en "Personal" y seleccionar "Siguiente".

The screenshot shows the 'Asistente para importación de certificados' window with the 'Almacén de certificados' tab selected. The text reads: 'Los almacenes de certificados son áreas del sistema donde se guardan los certificados.' Below this, it says: 'Windows puede seleccionar automáticamente un almacén de certificados, o bien es posible especificar una ubicación para el certificado.' There are two radio buttons: 'Seleccionar automáticamente el almacén de certificados en base al tipo de certificado' (unchecked) and 'Colocar todos los certificados en el siguiente almacén:' (checked). Below the radio buttons, there is a text box labeled 'Almacén de certificados:' with the word 'Personal' entered. To the right of the text box is a button labeled 'Examinar...'. At the bottom, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'.

- Luego seleccionar “Finalizar”. Windows muestra el mensaje de importación correcta.



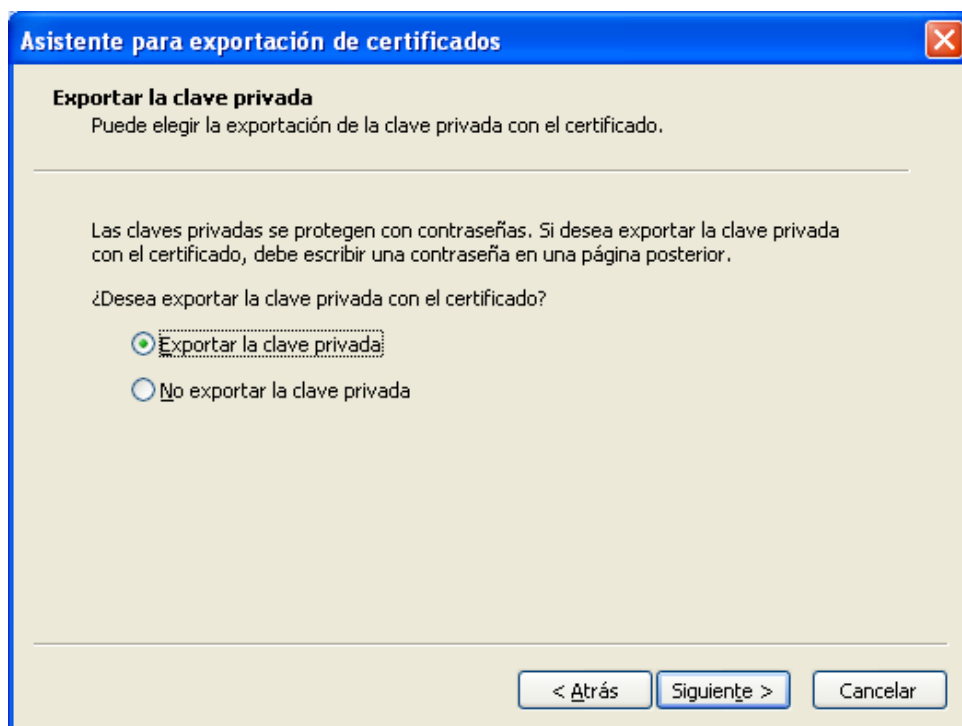
- Luego de Aceptar el mensaje, debe quedar algo como esto:



- En esta pantalla seleccionar el botón "exportar". Aparece el asistente.



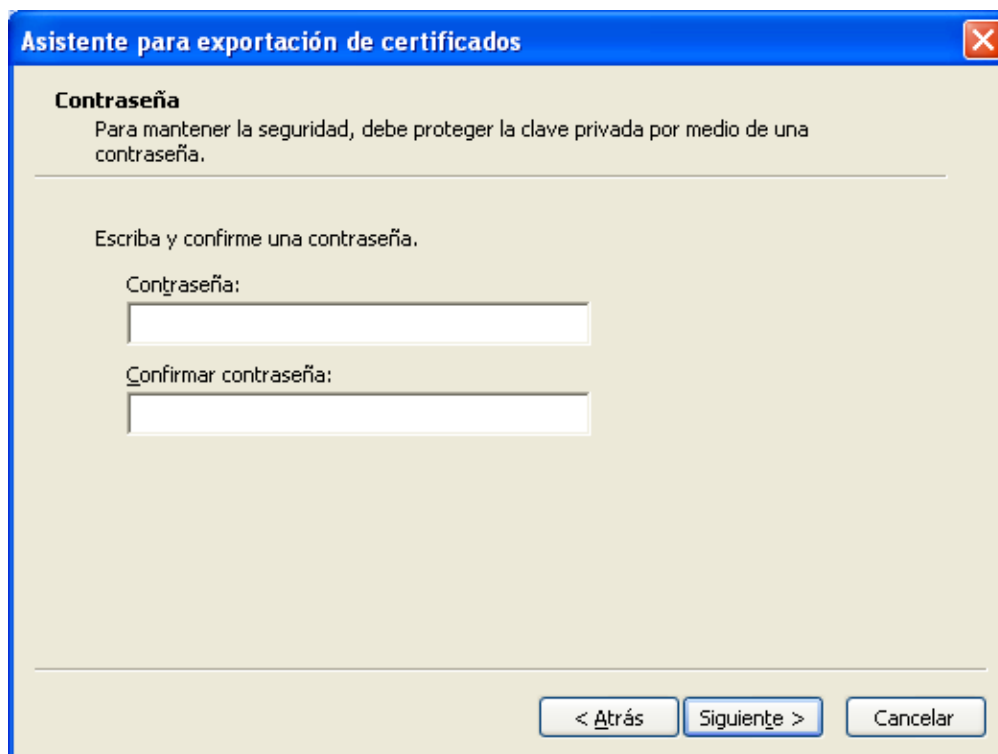
- En el asistente seleccionar "siguiente".
- Elegir "exportar la clave privada". Debe quedar como esto:



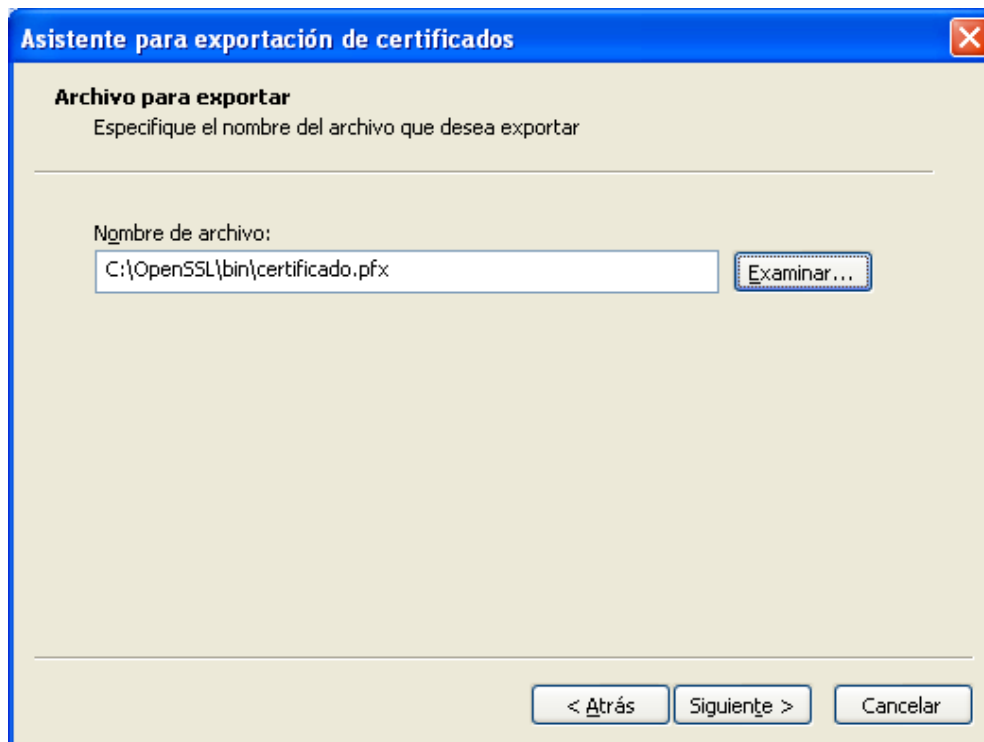
- Seleccionar "siguiente".
- En la pantalla que aparece dejar las opciones como están. Deberían ser estas:



- Seleccionar "Siguiente". Nos pedirá contraseña. no colocar nada.



- Seleccionar "Siguiente". Nos pedirá donde guardar el archivo (debemos ingresar el nombre del archivo) *.pfx. en la carpeta que lo guardemos (por ejemplo c:\OPENSSL\BIN\certificado.pfx).



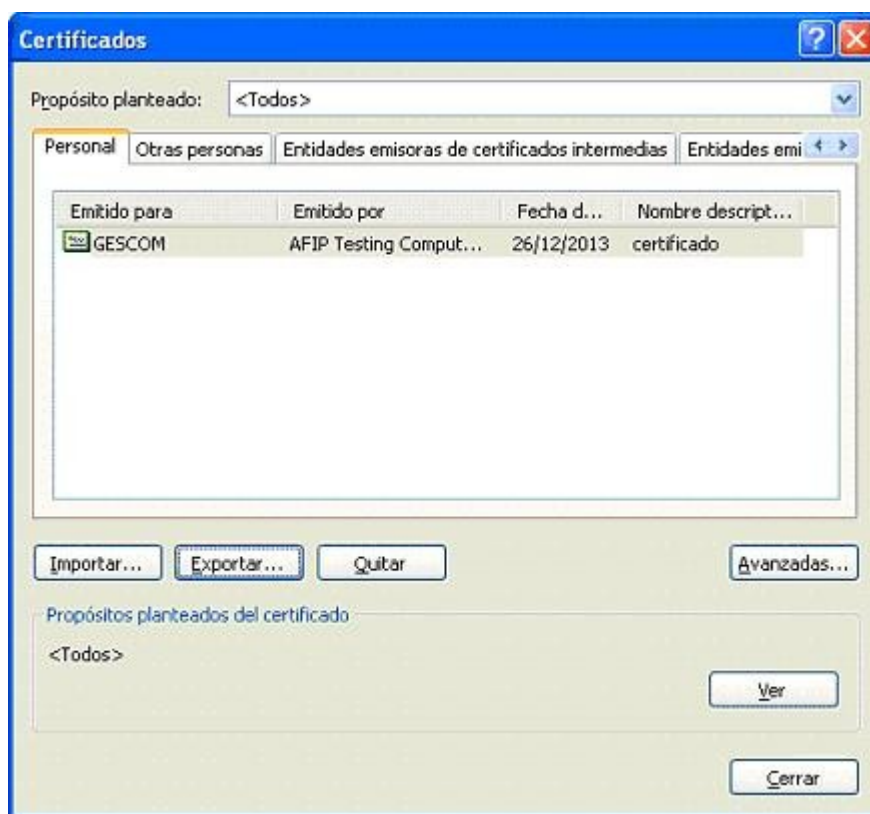
- Finalmente vemos la pantalla del asistente. Seleccionar “Finalizar”:



- Vamos a ver el siguiente mensaje, y con esto concluye la exportación:



- Al volver a la pantalla de CERTIFICADOS, seleccionar “Cerrar”.



En caso de inconvenientes, los servidores de la AFIP responderán con un mensaje que identifica el problema:

- ns1:coe.notAuthorized Computador no autorizado a acceder los servicios de AFIP: el certificado no es válido o no está correctamente asociado al ambiente en el cual se intenta usar (ej. certificado de homologación usado en producción). Revisar el proceso de generación y asociación del certificado.
- ns1:cms.cert.expired Certificado expirado: los certificados poseen una fecha de vencimiento que varía según el ambiente para el cual fueron creados y la fecha de emisión. Generar y asociar nuevamente el certificado.

OBS: Sincronización de Clocks: La fecha y hora del computador que se comunica con los servicios Web de AFIP deberá estar sincronizada. Dicha sincronización se podrá realizar a través del protocolo NTP con el servidor “time.afip.gov.ar” u otro servidor que preste dicho servicio.

ANEXO I – Solicitar y Obtener Certificado digital de AFIP para WSLPG - Web Service - Liquidación Primaria de Granos en modo producción (real).

Este documento describe el procedimiento para habilitar el consumo de Servicio Web de la AFIP, particularmente los correspondientes al servicio de Factura Electrónica (WSFE).

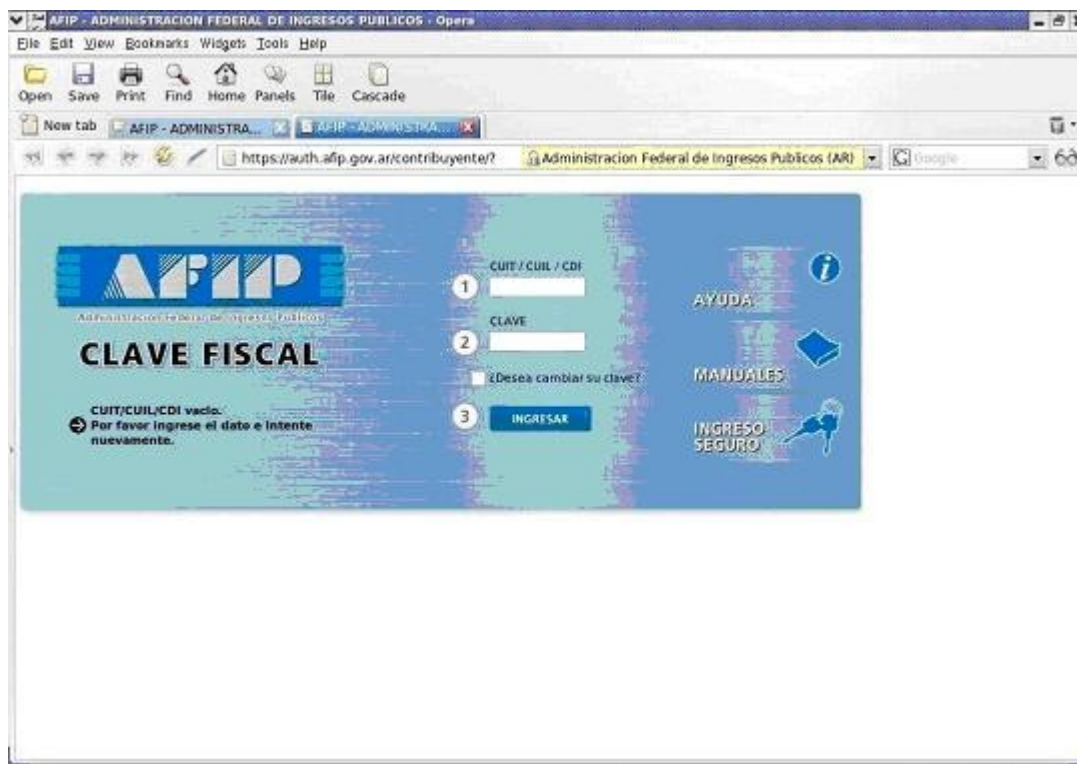
Para poder llevar a cabo este procedimiento, tanto la empresa que operará el Servicio Web como la empresa que facturará, deberán gestionar la obtención de una **Clave Fiscal de Nivel 3**, cuyo trámite deberá realizarse en una agencia de AFIP.

El siguiente Anexo tiene como objetivo mostrar los distintos pasos para la obtención de un certificado digital válido solamente para el entorno de producción.

PASO 1: Ingresar al portal de AFIP (www.afip.gov.ar) y presionar el botón < ir > sin completar ningún dato:



Se abre una nueva ventana con la página de acceso. Ingresar su “CUIT / CUIL / CDI” y “clave” y seleccionar “INGRESAR”:



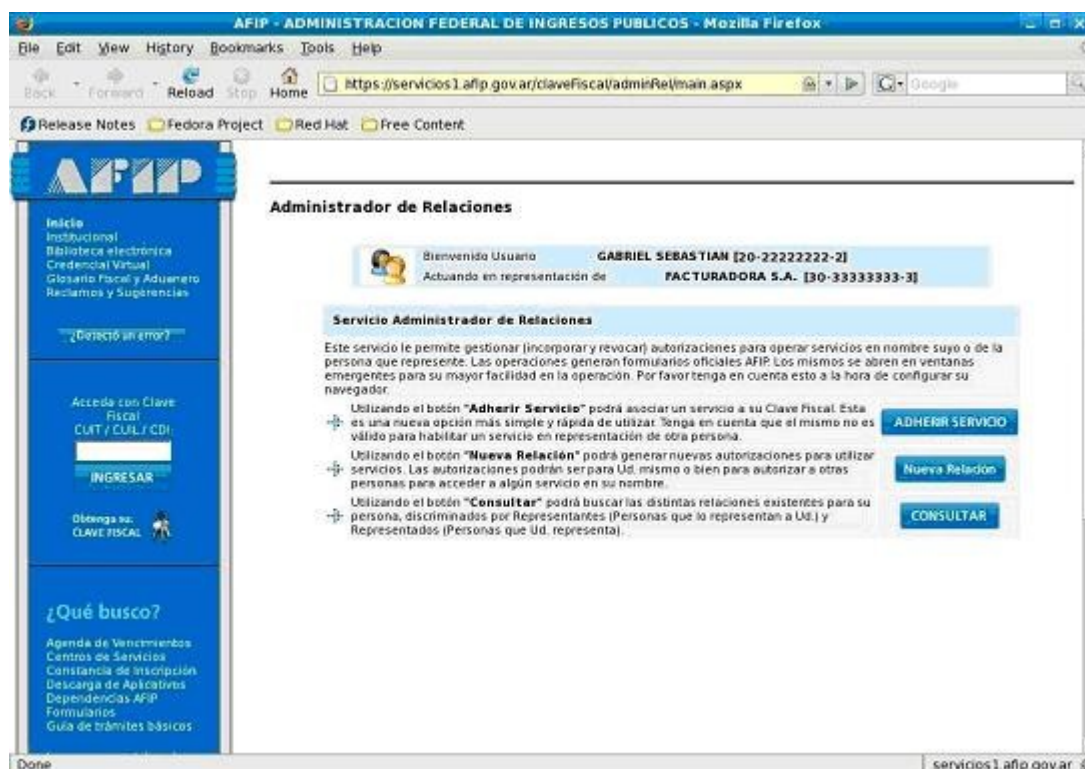
PASO 2: Luego en la siguiente lista de servicios seleccionar:

- a) Si está habilitado, seleccionar el servicio “Administración de Certificados Digitales”.
- b) Si el servicio “Administración de Certificados Digitales” no está habilitado, se debe seleccionar el servicio “Administrador de Relaciones de Clave Fiscal” (para poder habilitarlo).

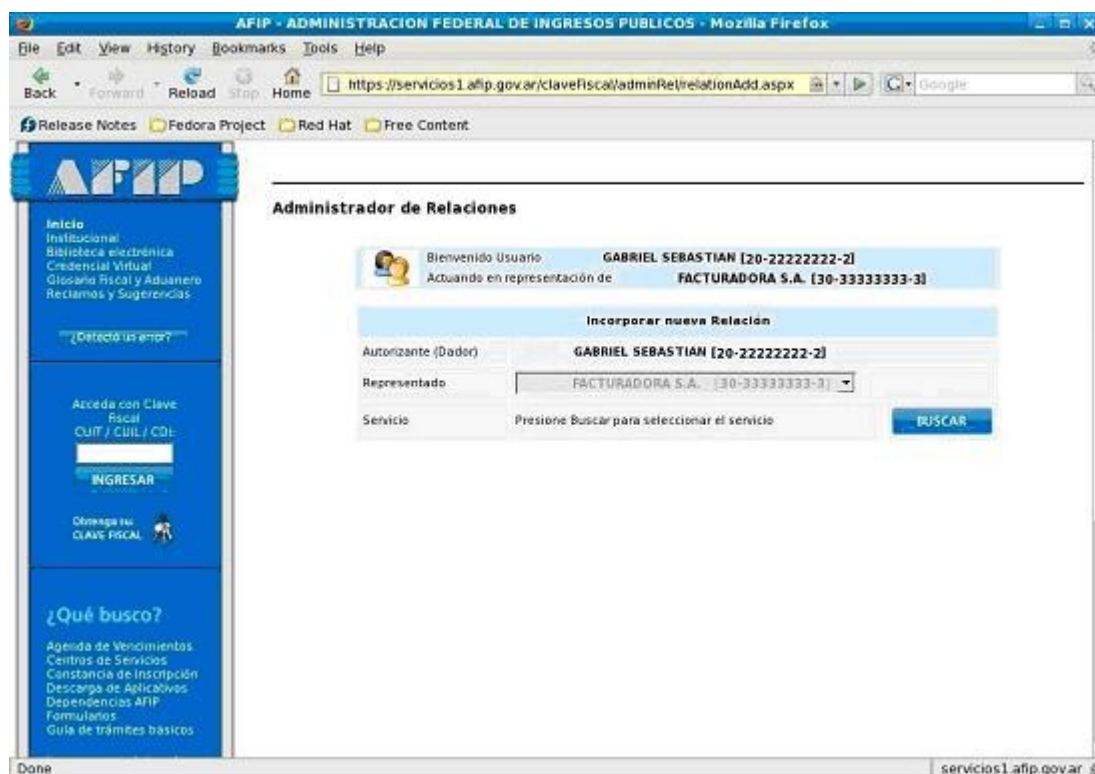


Si la opción es b) para poder habilitar el servicio “Administración de Certificados Digitales” se debe realizar lo siguiente:

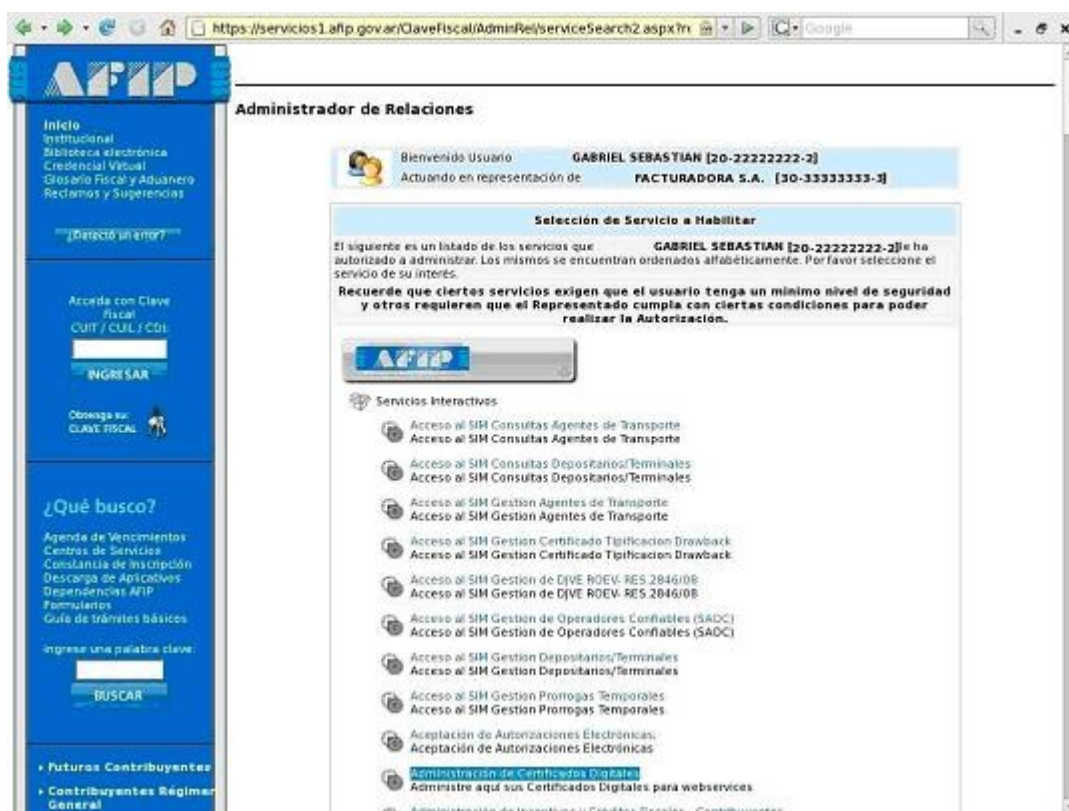
- Clickear en “Nueva Relacion”:



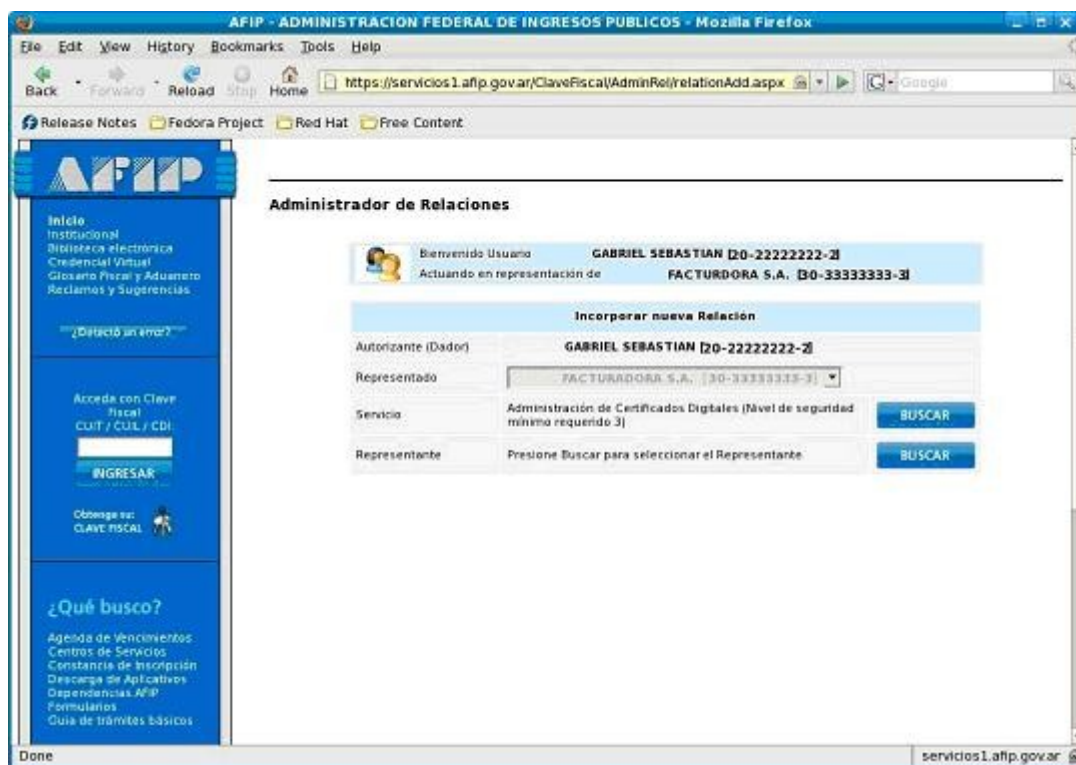
- Clickear en “BUSCAR” para seleccionar el servicio:



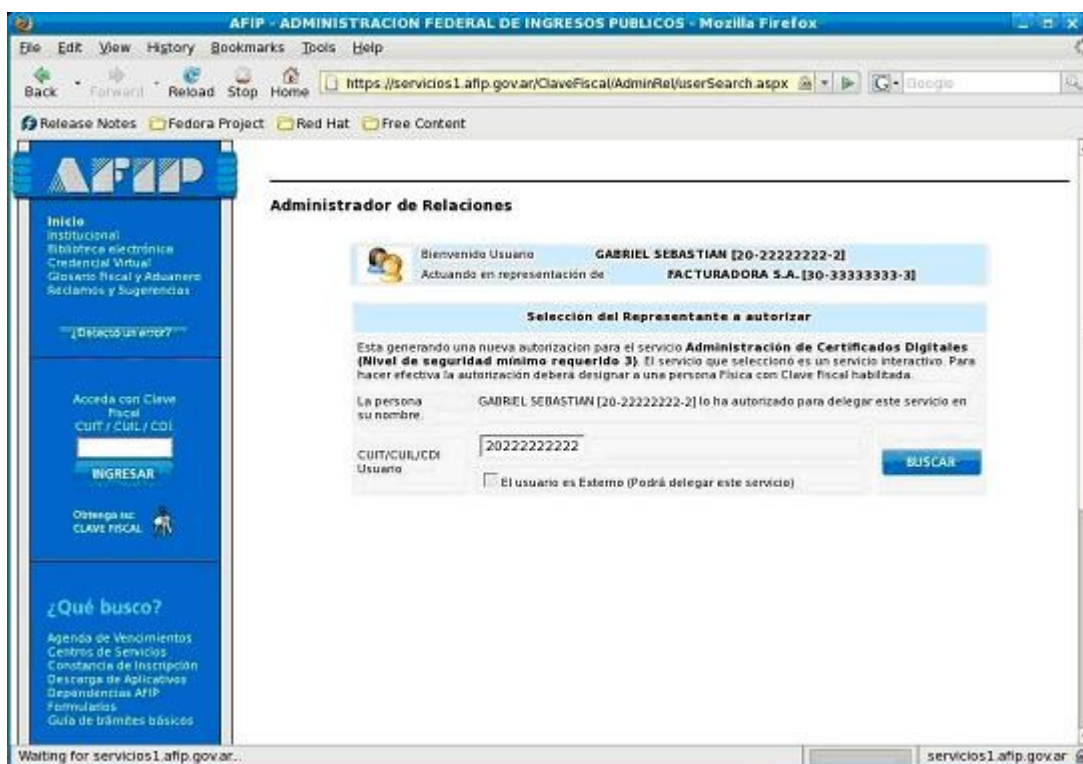
- Seleccionar el servicio “Administración de Certificados Digitales”:



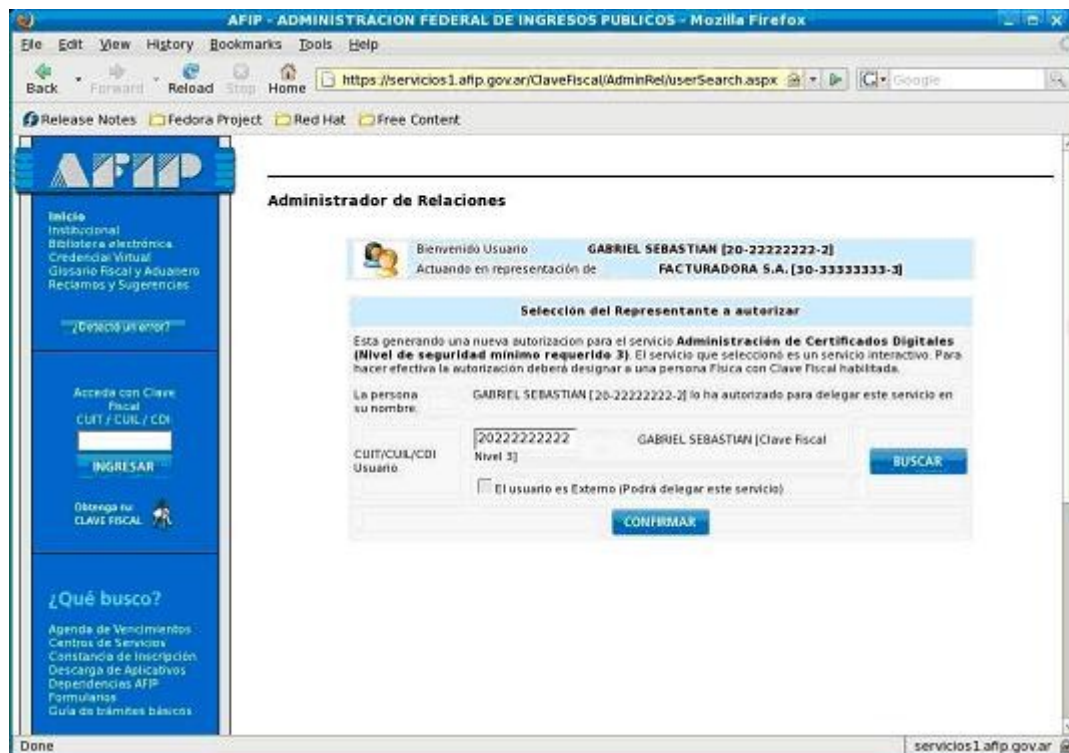
- Clickear en “BUSCAR” para seleccionar el Representante:



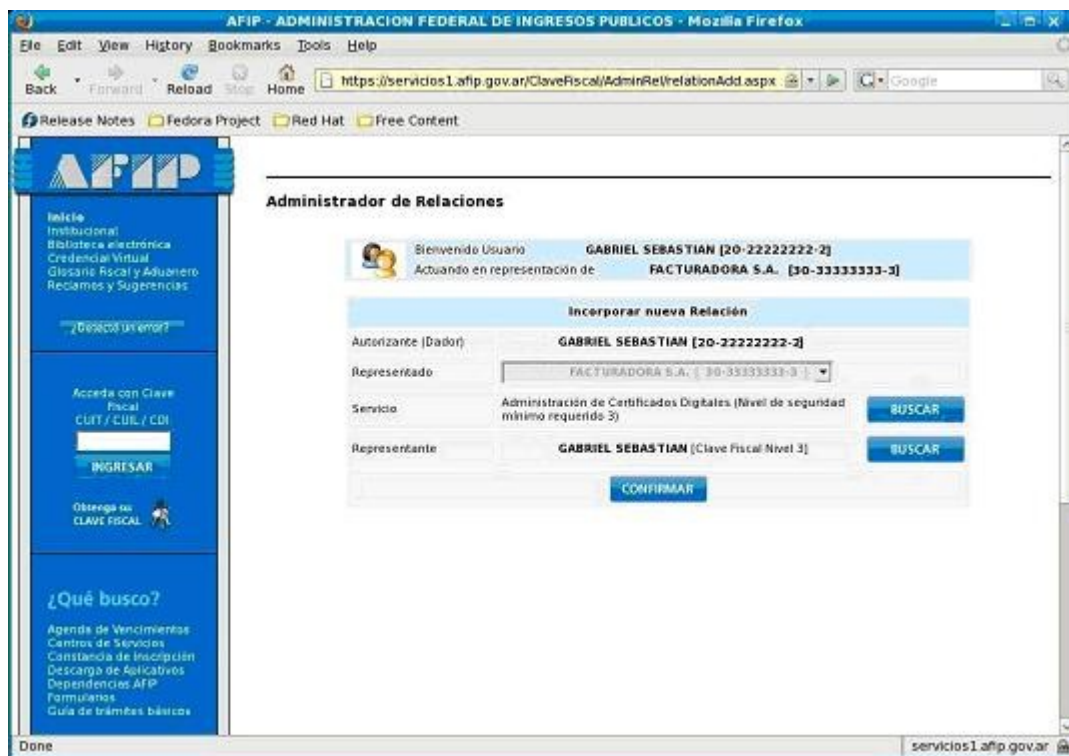
- Ingresar CUIT/CUIL/CDI del Representante y clicar en “BUSCAR”:



- Clicar en “CONFIRMAR”:



- Clickear en “CONFIRMAR”:



- Salir del sistema y volver a ingresar para poder visualizar y seleccionar el servicio “Administración de Certificados Digitales” en la lista de servicios.
- En caso de no visualizar el servicio en la lista, debe aceptar la relación utilizando el servicio “Aceptación de Designación”.

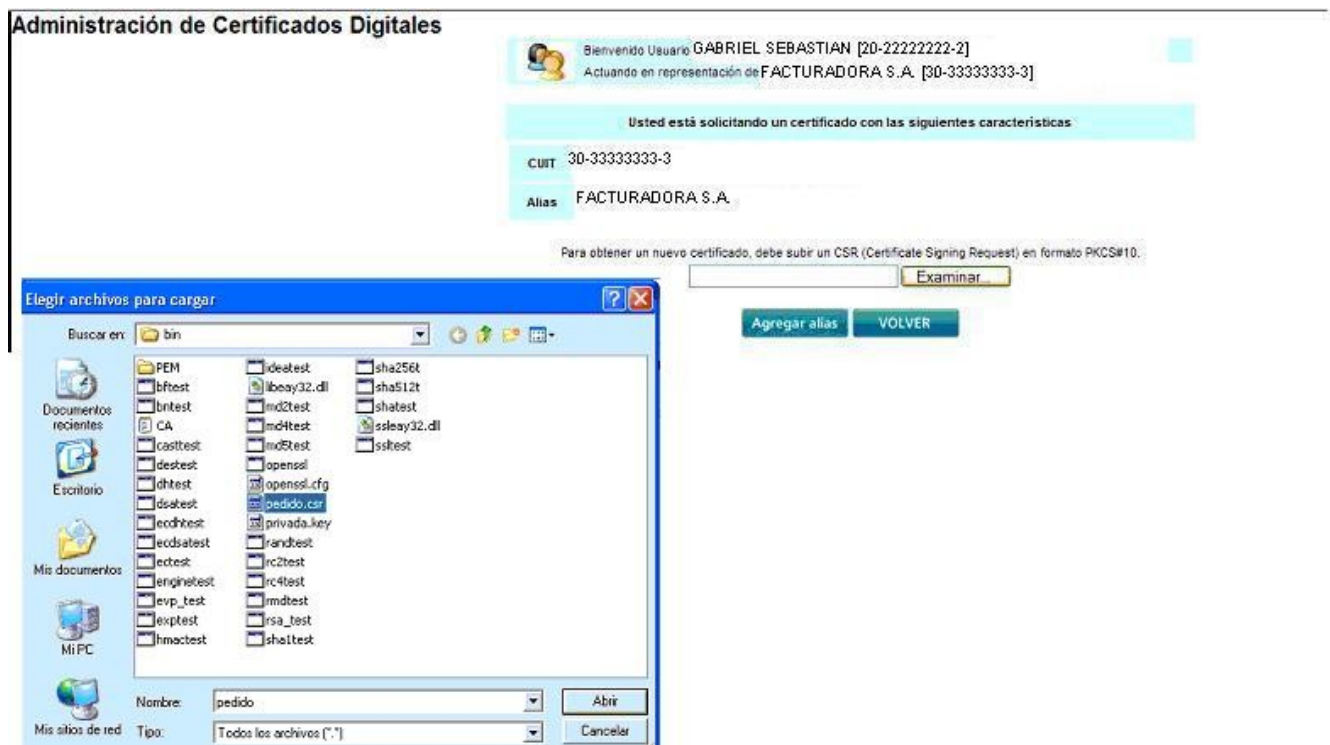
PASO 3: Una vez que ingresamos en “Administración de Certificados Digitales”, seleccionar el contribuyente para el que va a operar el servicio (si representa a más de un contribuyente):



PASO 4: Hacer click en “Agregar alias”:




PASO 5: Hacer click en Examinar para subir el archivo de extensión CSR generado en los pasos previos con los comandos del OPENSSL (en nuestro ejemplo habíamos generado el archivo pedido.csr en la carpeta \OPENSSL\BIN). Luego cliquear en “Agregar alias”:




PASO 6: Hacer click en “Descargar”, para poder descargar a su PC el certificado, que será un archivo con extensión **crt** que nos va a permitir continuar con la habilitación y utilización de los servicios Web de AFIP.

Administración de Certificados Digitales

 Bienvenido Usuario **GABRIEL SEBASTIAN** [20-22222222-2]
Actuando en representación de **FACTURADORA S.A.** [30-33333333-3]

CUIT 30333333333
Alias FACTURADORA S.A.
DN C=ar, ST=some-state, O=FACTURADORA SERIALNUMBER=CUIT3033333333, CN=comisi

Nro Serie	Fecha Emision	Fecha Vencimiento	Estado	Descargar
362306d95ef71b36	2/28/2013 1:50:23 PM	3/1/2015 1:50:23 PM	VALIDO	

[Agregar certificado](#) [VOLVER](#)

PASO 7: Volver a ingresar a la página del Afip, con clave fiscal. Ir a Administración de Relaciones de Claves Fiscal, elegir Afip, luego Web Services, y ahí elegir el web service al que se quieren adherir:

WSFE – Web Service de Factura Electrónica

WSFEX- Web Service de Factura Electrónica de Exportación

WSBFE – Web Service de Factura Electrónica bonos fiscales y bienes de capital

WSMTXCA – Web Service Factura Electrónica con Detalle

WSCTG – Web Service Código de Trazabilidad de Granos

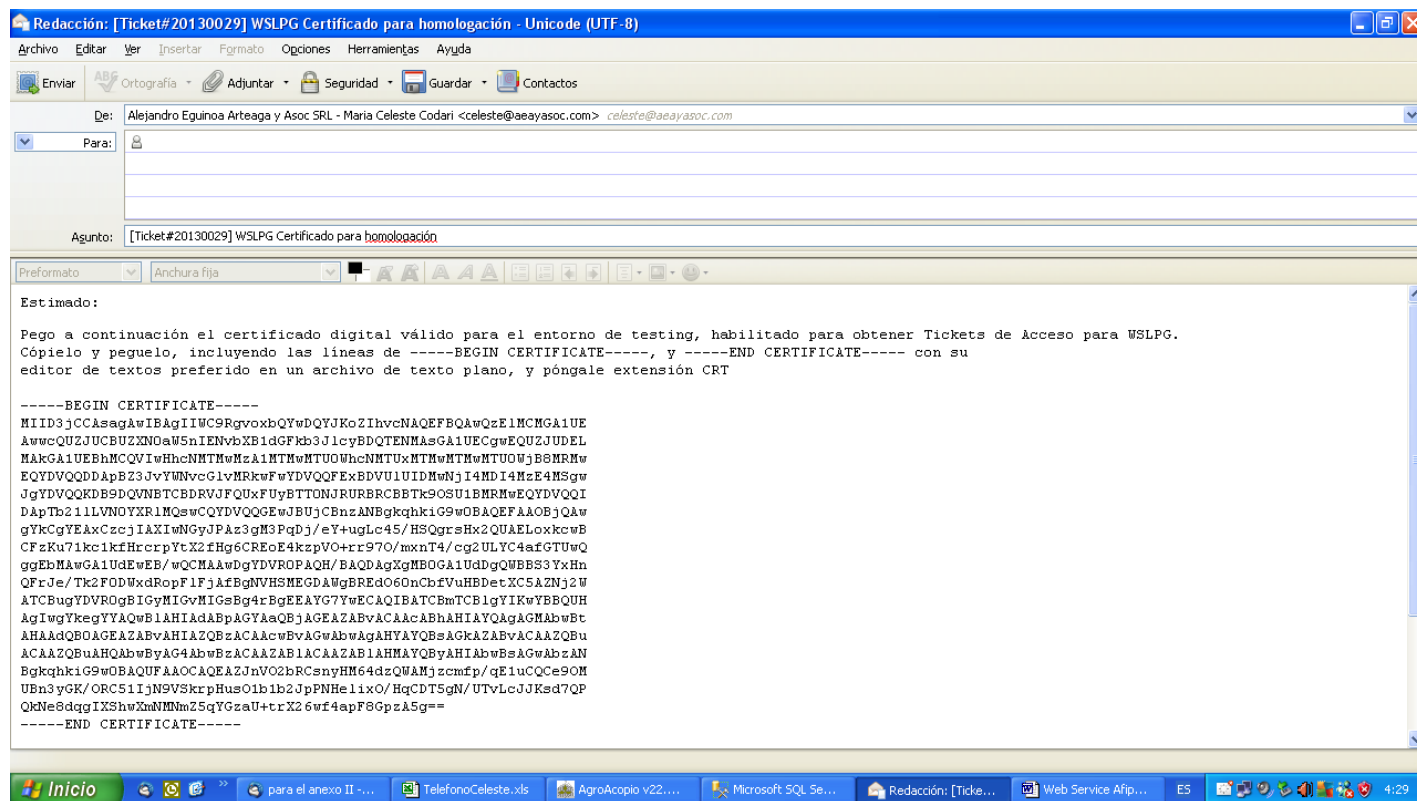
WSLPG - Web Service - Liquidación Primaria de Granos

ANEXO II– Solicitar y Obtener Certificado digital de AFIP para WSLPG - Web Service - Liquidación Primaria de Granos en modo Homologación (prueba).

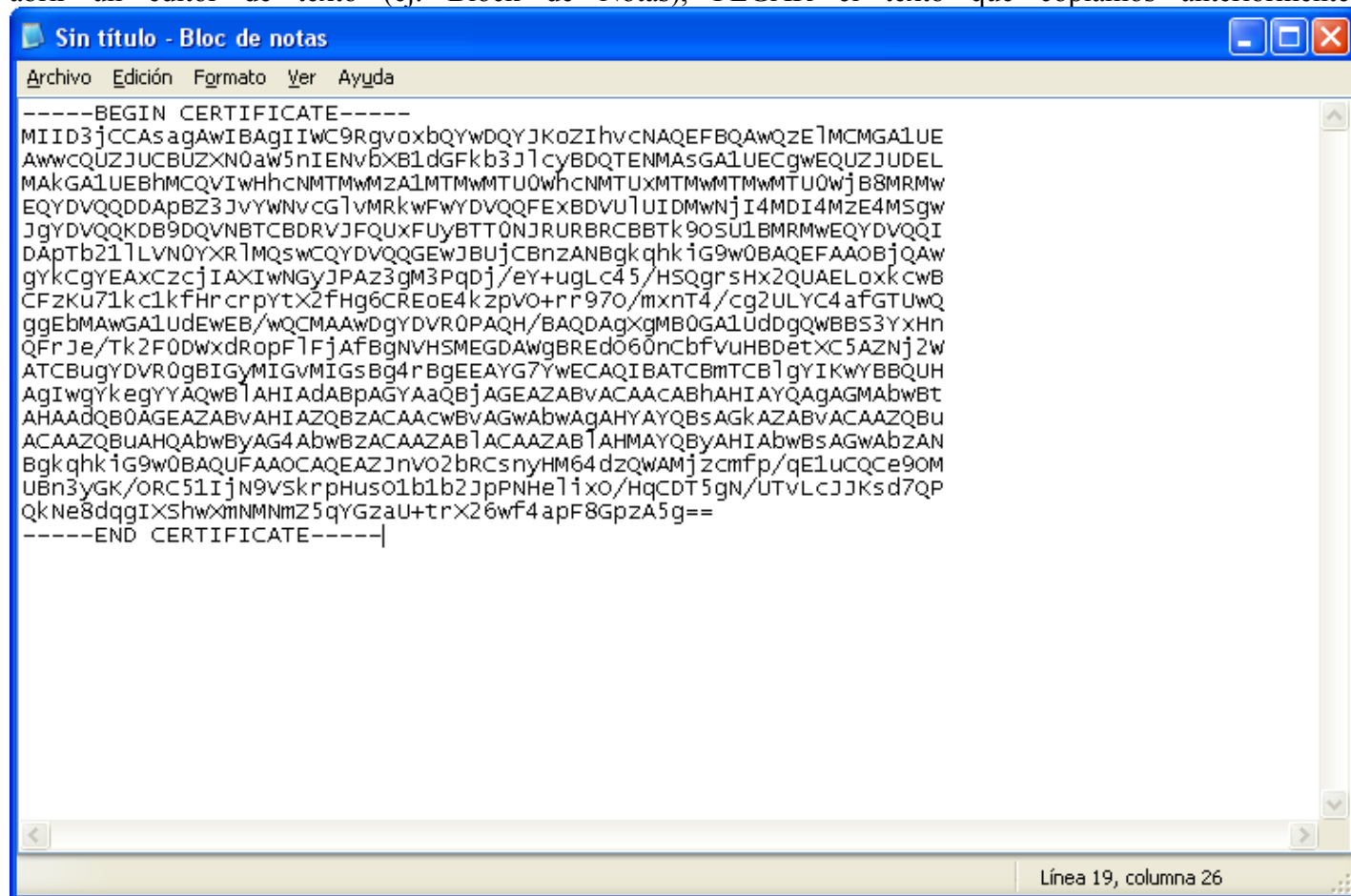
Enviar un mail a webservices@afip.gob.ar, solicitando a la AFIP la Homologación para poder usar el Web Service en modo de Prueba.

Luego AFIP responderá el mail con los datos del certificado digital válido para el entorno de testing (Prueba), habilitado para obtener Tickets de Acceso para WSLPG.

El mail que recibiremos de AFIP tendrá un formato similar al que se detalla a continuación:



Seleccionar el texto desde -----BEGIN CERTIFICATE-----, y -----END CERTIFICATE-----, COPIARLO, abrir un editor de texto (ej. Block de Notas), PEGAR el texto que copiamos anteriormente.

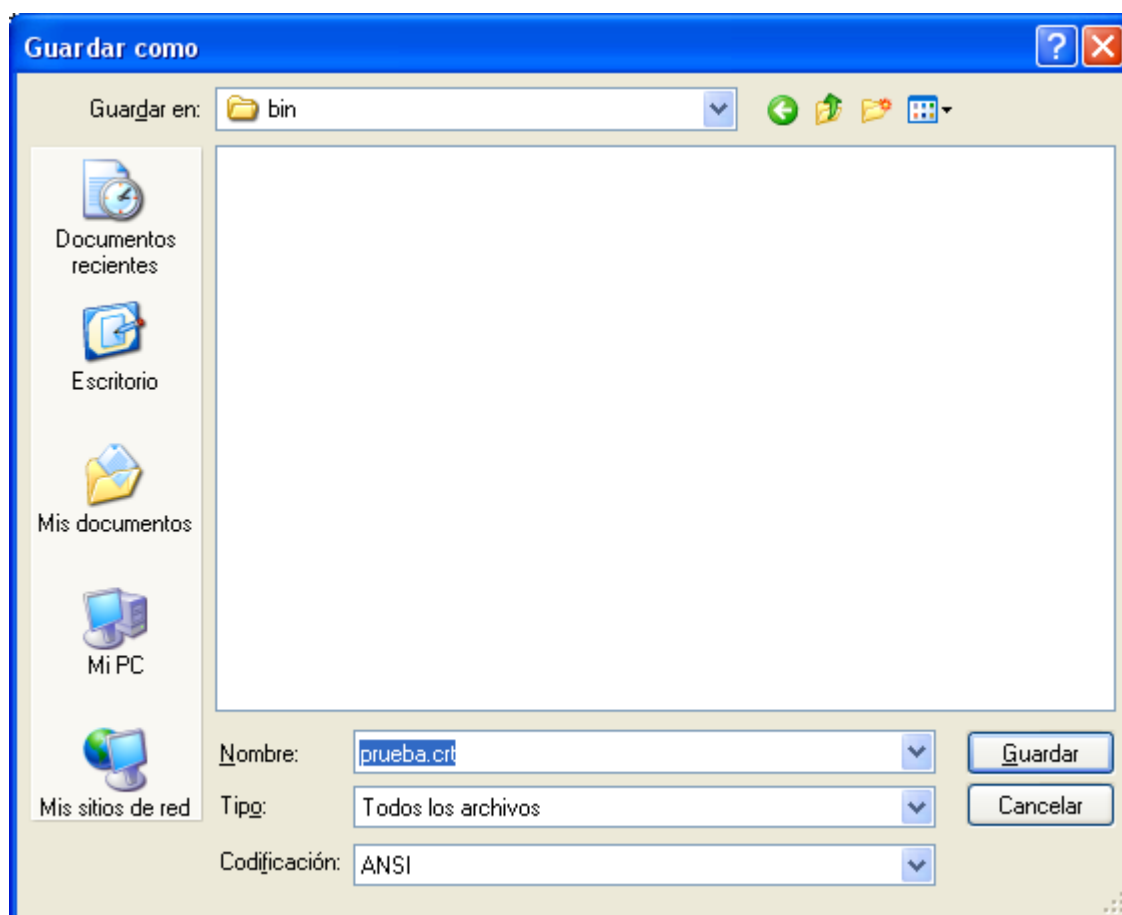


```

-----BEGIN CERTIFICATE-----
MIID3jCCAsagAwIBAgIIWC9RgvoxbQYwDQYJKoZIhvcNAQEFBQAwQzElMCMGA1UE
AwwcQUZJUCBUZXN0aw5nIENvbXB1dGFKb3JlcyBDQTenMASGA1UECgwEQUZJUDEL
MAKGA1UEBhMCQVwHhcnMTMwMZA1MTMwMTU0WncNMTUxMTMwMTMwMTU0WjB8MRMw
EQYDVQQDDApBZ3JvYWNvcmVzMRkwFwYDVQQFEExBZDU1UjBMDI4MZE4MSgw
JgYDVQQKDB9DQVNBTCBDRVJFQUxFUyBTT0NJRURBRCBBTk90SU1BMRMwEQYDVQQI
DAptb21lLVN0YXRlMQswCQYDVQQGEwJBUjCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYKCgYEAXCZcjIAXIwNGYJPAZ3gM3PqDj/eY+ugLc45/H5QgrsHx2QUAELoxkcwB
CFzKU71kc1kfHr crpytX2fHg6CREoE4kzpvo+rr970/mxnT4/cg2ULYC4afGTUwQ
ggEbMAWGA1UdEwEB/wQCMAAwDgYDVR0PAQH/BAQDAgXgMB0GA1UdDgQWBBS3YxHn
QFrJe/Tk2F0DwxdropF1FjAFBgNVHSMEGDAwgbREd060nCbFvUHBDeTXC5AZNj2W
ATCBugYDVR0gBIGyMIGVMIGSBg4rBgEEAYG7YwECAQIBATCBMTCB1gYIKwYBBQUH
AgIwgYKegYYAQwB1AHIAAdABPAGYAaQBjAGEAZABVACAACABHAIAYQAgAGMAbwBT
AHAAQDQ0AGEAZABVAHIAZQBZACAACwBvAGwAbwAgAHYAYQBSAGkAZABVACAQZBU
ACAAZQBUAHQAAbwByAG4AbwBZACAABZAB1ACAAZAB1AHMAYQByAHIAbwBsAGwAbZAN
BgkqhkiG9w0BAQUFAAOCAQEAZJnvo2bRCSnyHM64dzQWAMjzcmfp/qE1uQCce9OM
UBN3yGK/ORC51IjN9VSkRphus01b1b2JpPNHelixO/HqCDT5gn/UTvLcJJksd7QP
QkNe8dggIXShwxmNMNmZ5qYGZaU+trX26wf4apF8Gpza5g==
-----END CERTIFICATE-----

```

Guardarlo en la carpeta \OpenSSL\bin con el nombre que desee y de extensión “crt”.



Una vez finalizado continuar con el PASO 4.